UDC 338.27:004.056(4-67)
JEL E02, O33, G32, L86
DOI 10.32782/2786-765X/2025-11-7

Alona Buriak
PhD in Economics, Associate Professor of the Department
of International Economic Relations and Tourism,
National University "Yuriy Kondratyuk Poltava Polytechnic"
Oleksandra Maslii
PhD in Economics, Associate Professor of the Department
of Finance, Banking and Taxation,
National University "Yuriy Kondratyuk Poltava Polytechnic"

EUROPEAN APPROACHES TO ENHANCING THE STATE'S ECONOMIC SECURITY THROUGH THE DEVELOPMENT OF CYBER RESILIENCE

The article substantiates the conceptual foundations of strengthening a state's economic security through the development of cyber resilience in the context of digital transformation. The European experience of implementing NIS2, DORA, GDPR, and the Cyber Resilience Act is summarized as the regulatory basis for the EU's digital economy stability. A comparative analysis of the cyber resilience systems of the EU and Ukraine reveals institutional asymmetry but dynamic harmonization progress. The study proposes a conceptual model for enhancing economic security through the integration of European cyber resilience practices into national governance, emphasizing strategic priorities for aligning Ukraine's cybersecurity legislation and creating a digital risk management system. The practical value of the results is reflected in strategic priorities for harmonizing Ukraine's cybersecurity legislation with EU norms.

Keywords: economic security, cyber resilience, information security, security-oriented information environment, digital risks.

Problem statement. The digital transformation of Europe's economic systems has necessitated a shift from traditional cybersecurity models to a cyber resilience paradigm, which encompasses not only threat prevention but also adaptation and rapid recovery after incidents. In the contemporary context, cyber resilience has become a defining element of economic security, as the stability of financial, energy, and industrial systems depends on the ability of states and businesses to maintain the uninterrupted operation of digital infrastructure. For Ukraine, currently in a state of hybrid warfare, enhancing cyber resilience is of strategic importance, as cyberattacks directly impact macroeconomic stability, investor confidence, and EU integration processes.

Analysis of recent research and publications. In contemporary scientific and analytical research, there is an active rethinking of approaches to ensuring the economic security of the state through the development of cyber resilience systems. According to the ENISA Threat Landscape 2024 report, the number of sophisticated attacks on critical infrastructure is increasing, while the range of targeted sectors now includes energy, transport, and finance. The European Union Agency for Cybersecurity emphasizes the need to strengthen multi-level response mechanisms, harmonize regulatory frameworks, and enhance the role of education and digital competencies in reinforcing the resilience of the digital economy [2].

A significant contribution to the scientific foundations of risk assessment was made by Aghazadeh Ardebili A., Lezzi M. and Pourmadadkar M. [1], who developed a methodology for analyzing cyber risks in critical infrastructures, considering the interaction of technical, organizational, and regulatory factors. The authors demonstrated the effectiveness of combining NIS2 standards with cyber risk management models to enhance the resilience of socio-technical systems.

Similar conclusions are presented in the study by Cho H., Sung J.-H., Kang H.-J., Jang J., & Shin D. [5], which proposes a quantitative framework for assessing cyber resilience based on system availability metrics and AUC-based normalization. This approach enables objective comparisons of resilience levels across different economic sectors and supports strategic planning in digital security.

From a regulatory perspective, the study by Ristvej J., Tonhauser M., Chovanec D. et al. [7] focuses on the implementation of NIS2 standards in EU member states. The conceptual model developed by the authors integrates a risk-oriented

approach into public governance, promotes the establishment of interagency coordination centers, and advances systematic monitoring of cyber incidents.

The research by Coppolino L., Nardone R., Petruolo A., Romano L. & Souvent A. [11] highlights the potential of digital twin technology for cybersecurity monitoring in smart energy grids. By combining big data analytics with real-time modeling, this technology improves anomaly detection accuracy and reduces response time to cyber incidents.

Another important research direction involves the ethical and applied aspects of cybersecurity. Timothy C Haas [3] argues for the adaptation of cybersecurity practices to counter wildlife-related cybercrime, emphasizing the interdisciplinary nature of modern cyber policy and the necessity of considering the socio-economic implications of digital risks.

At the empirical level, important data are provided in the annual CERT-UA reports, which summarize cyber incident statistics, trends in the development of Ukraine's national cybersecurity system, and directions of cooperation with EU institutions [6]. Data from Eurostat also show an increasing share of enterprises implementing cyber resilience policies, along with higher investments in digital security and workforce skills [4].

Therefore, the analysis of international and national studies from 2023–2025 indicates an evolution of the cyber resilience concept – from a purely technical component of security to a comprehensive socio-economic phenomenon. The European model, based on the principles of NIS2 and ENISA, demonstrates the effectiveness of integrating regulatory requirements, analytical tools, and technological innovations to strengthen the economic security of states in the digital environment.

The aim of the article. The aim of the article is to summarize European experience in shaping cyber resilience as a system-forming factor of a state's economic security and to justify directions for adapting its key institutional and regulatory mechanisms to domestic practice.

Presentation of the main research material. The digitalization of the European space has created the prerequisites for a new paradigm of economic security – security based on cyber resilience. This paradigm involves not only the technical ability to counter cyberattacks but also the institutional, financial, and educational readiness of states and enterprises to ensure the stability of the digital economy.

In the current context, a state's economic security increasingly depends on the capacity of national institutions to counter cyber aggression, preserve the integrity of financial data, and ensure the continuity of economic processes. The European Union has developed an integrated system of approaches to cyber resilience, encompassing legal regulation, institutional coordination, investment mechanisms, and the development of digital competencies among the population.

According to research findings [8], Ukraine's security environment is closely linked to the dynamics of European integration processes, and the implementation of EU cyber resilience standards is a strategic condition for sustainable economic development.

The term "cyber resilience" in European academic discourse is defined as the ability of a state, organization, or system to withstand, adapt to, and rapidly recover from cyber incidents while ensuring the continuity of core functions. Unlike the concept of "cybersecurity," which focuses on threat prevention, cyber resilience includes post-crisis recovery and organizational learning. According to the EU Cybersecurity Strategy 2020 [2], cyber resilience comprises three components:

1. Anticipation of risks.
2. Protection and deterrence.
3. Recovery and adaptation.

Researchers [12] emphasize that in today's global conditions, cyber resilience is the foundation of national financial stability, as the financial system is one of the most vulnerable elements of the digital environment. It ensures shock resistance only through the interaction of state, corporate, and international levels of governance.

Within the framework of a state's economic security, the cyber resilience system is considered a multi-component structure that integrates legal, technological, organizational, and social elements interacting within a unified information-analytical space (Fig. 1).

The coordinated interaction of these components ensures a synergistic effect, manifested in the reduction of the economic system's vulnerability, the enhancement of the investment attractiveness of the digital environment, and the formation of a national continuum of cyber-economic security.

The European cyber resilience system is multi-level and involves integration across the supranational level, through the activities of the European Union Agency for Cybersecurity (ENISA); the national level, through the implementation of the NIS2, DORA, and GDPR directives; and the sectoral level, through industry-specific standards (Table 1).

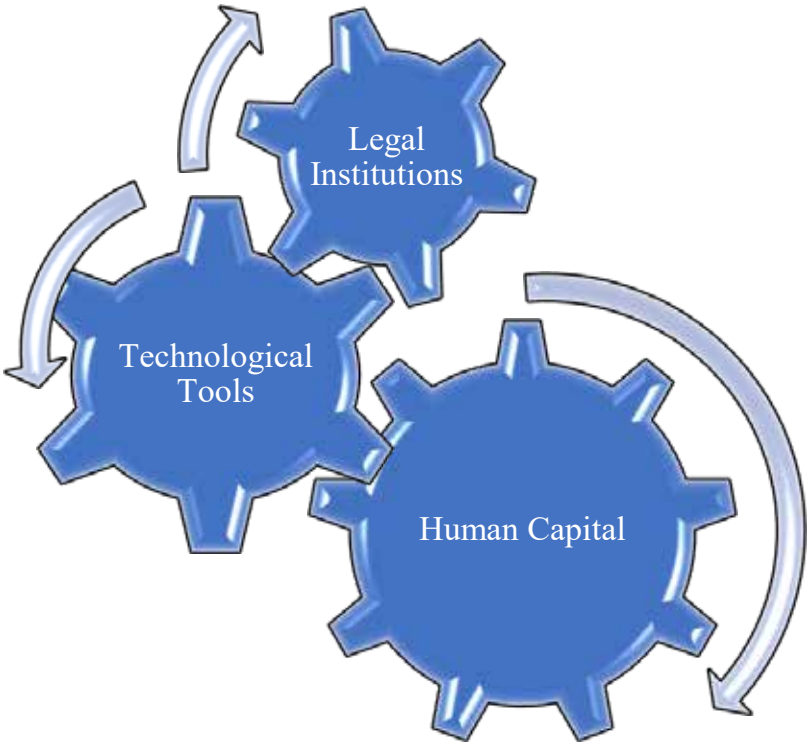

Fig. 1. Conceptual structure of cyber resilience within the economic security system

Source: compiled based on data from [2, 8]

Table 1

Key elements of the European cyber resilience system

Level	Key Institutions / Regulations	Functions	Expected Effect
Supranational	European Commission, ENISA, CERT-EU	Policy development, monitoring, and support for member states	Standards harmonization
National	Cybersecurity Agencies of EU Member States	Directive implementation and coordination of crisis response actions	Incident reduction
Sectoral	Banking, energy, and transport regulators	Critical infrastructure protection	Enhancing sectoral cyber resilience
Educational / Human Resources	European Academy of Cybersecurity	Training of specialists and skills development	Growth of digital culture

Source: compiled based on data from [2, 4]

According to estimates by the European Commission and the European Union Agency for Cybersecurity (ENISA), in 2024–2025, EU member states' investments in cybersecurity average 0,8% of GDP, corresponding to approximately €145 billion per year. This level of funding ensures not only the stability of critical infrastructure operations but also enhances the technological autonomy of the EU's digital economy.

Around 42% of the funds are allocated to the creation of early warning and cyber threat monitoring systems, 27% – to educational and research programs for the development of human capital in cybersecurity, 18% – to innovative projects and public-private partnerships, and 13% – to regulatory and analytical activities as well as coordination measures by ENISA and national CERT structures (Fig. 2).

This approach demonstrates the prioritization of investments in preventive mechanisms that reduce the vulnerability of digital infrastructure to crisis situations and foster the long-term economic resilience of the EU. At the same

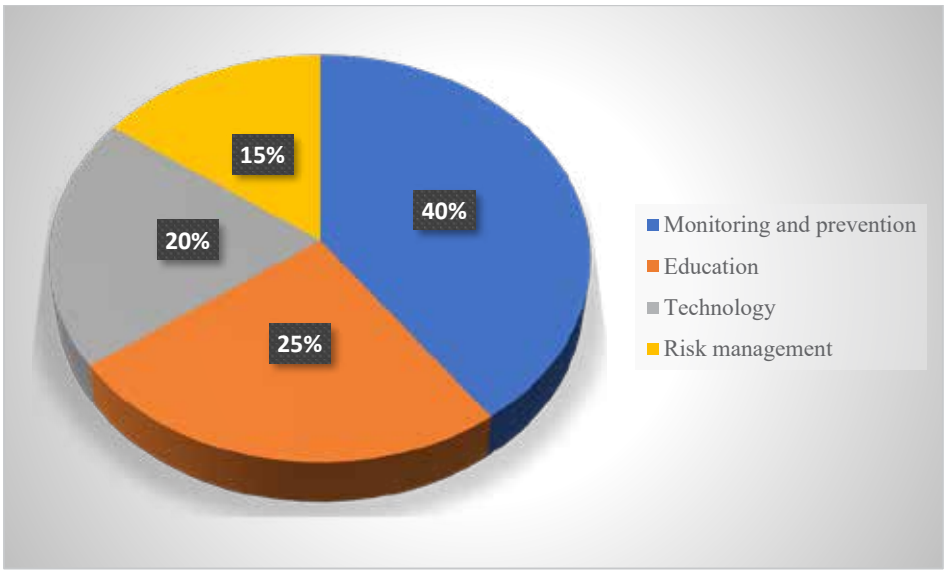

Fig. 2. Structure of funding for cybersecurity resilience measures in the EU, % of GDP

Source: compiled based on data from [2, 6]

time, these data reflect the shift from a reactive cybersecurity model to a proactive cyber-resilience system based on big data analytics, artificial intelligence, and distributed analytical platforms.

The main mechanisms for shaping and ensuring the cyber resilience of EU member states are systematized in Table 2 across four fundamental directions, reflecting the integrity of the European digital risk management model.

The first is the regulatory and normative direction, which ensures legal certainty and the unification of requirements for the protection of critical digital infrastructures. Key acts include the NIS2 Directive (2022), which expands the scope of responsibility for operators of essential services and digital service providers; the DORA Regulation (2023), aimed at enhancing the operational resilience of the financial sector; and GDPR (2018), which establishes a unified legal framework for personal data protection within the EU digital space.

The second is the institutional direction, represented by the activities of the European Union Agency for Cybersecurity (ENISA), the network of national CERT-EU response centers, and the European Cybersecurity Competence Centre (ECCC), which form a networked architecture for operational response, information exchange, and strategic forecasting of cyber threats.

The third is the financial and investment direction, implemented through programs such as Digital Europe, Horizon Europe, and the Connecting Europe Facility, aimed at stimulating security innovations, creating data-sharing infrastructure, and introducing new solutions in artificial intelligence, cloud technologies, and blockchain sectors.

The fourth is the educational and communication direction, which encompasses the development of digital academies, cybersecurity competence centers, and training networks that ensure the growth of digital culture, professional skills, and public awareness of cyber risks.

Thus, the cyber resilience mechanisms in the EU are integrated, combining legal, organizational, institutional, and educational support with financial incentives for digital

Table 2

Mechanisms for strengthening the cyber resilience of EU member states

Mechanism	Implementation tool	Example	Outcome
Regulatory	NIS2 Directive	France: Development of the SOC Network	Coordination of crisis responses
Institutional	ENISA, CERT-EU	Germany: National Cyber Center	Reduction of attacks by 22%
Financial	Digital Europe Program	Spain: SmartCyber 2024	Increase in investments by 35%
Educational	European Cybersecurity Academy	Poland: E-Resilience Initiative	Enhancement of cybersecurity literacy

Source: compiled based on data from [2, 4]

security development, creating preconditions for the sustainable functioning of economic systems in high-risk environments.

A determining factor distinguishing EU and Ukrainian cyber resilience systems is the level of institutional maturity and the comprehensiveness of risk management approaches. In EU countries, cyber resilience is integrated at all levels of economic governance – from national to municipal. In Ukraine, as noted by researcher [10], the process of digitally strengthening security is fragmented and only gradually becoming systemic. A comparative characterization of the cyber resilience systems of the EU and Ukraine is presented in Table 3.

The results indicate a gradual convergence of the cyber resilience systems of the EU and Ukraine; however, institutional and resource

Table 3

Comparative characteristics of EU and Ukrainian cyber resilience systems

Comparison criterion	European Union	Ukraine	Analytical commentary
Strategic basis of cybersecurity	EU Cybersecurity Strategy (2020–2030), aligned with digital sovereignty and data security policies	Ukraine Cybersecurity Strategy (2021-2025); concept of integration into the EU digital market	Both strategies share common directions; however, Ukraine lags behind in the implementation of NIS2 and GDPR standards
Institutional architecture	ENISA, CERT-EU, European Cybersecurity Competence Centre (ECCC), network of national CSIRTs	State Service of Special Communications, CERT-UA, NSDC, Ministry of Digital Transformation, National Cybersecurity Center	The EU has well-developed interstate coordination, whereas in Ukraine there is a national focus and a need to develop regional hubs
Regulatory and legal framework	NIS2 Directive (2022), DORA Regulation (2023), GDPR (2018)	Law "On the Basic Principles of Ensuring Cybersecurity of Ukraine," draft law "On Cyber Resilience" (2025)	The EU ensures mandatory implementation of directives, whereas Ukraine is gradually harmonizing its regulations with European law
Cybersecurity funding	Average level – 0,8% of GDP, including programs such as Digital Europe and Horizon Europe	Approximately 0,3% of GDP, programs such as EU4Digital and the Digital Recovery Plan	The funding gap is narrowing thanks to donor programs and international technical assistance
Cyber education and human capital	Networks such as the European Cybersecurity Academy, CyberSkills4All, and national competence centers	CyberSchool UA, regional courses by the Ministry of Digital Transformation, "Drone Army" programs	The EU has a well-established educational ecosystem, whereas Ukraine is rapidly developing specialized training programs but lacks systemic coherence
Incident monitoring and response	Joint Cyber Unit system, network of SOCs and CERTs in EU member states	Cyber Incident Response Center at the State Service of Special Communications, CERT-UA	Ukraine is actively developing operational monitoring; however, it requires broader analytical information exchange with the EU
International integration	Single Digital Market, Cyber Solidarity Act, participation in NATO CCDCOE global initiatives	Participation in EU4Digital programs, Cyber Rapid Response Teams, cooperation with ENISA	The level of international coordination is increasing; it is important to ensure political continuity of the integration process
Cyber Resilience Index (2025)	0,81	0,68	Ukraine demonstrates a steady positive trend toward approaching the EU average level
Level of digital competencies of the population (2025)	73%	62%	Digital literacy is increasing; however, additional educational and communication measures are required
Type of risk management	Preventive-analytical with elements of automated threat assessment	Reactive-preventive with gradual implementation of forecasting tools	The EU focuses on prevention, whereas Ukraine emphasizes minimizing the consequences of incidents

Source: compiled based on data from [2, 8–9]

asymmetries remain. Ukraine demonstrates dynamic growth in the cyber readiness index but requires strengthening of human resources, increased funding, and implementation of comprehensive preventive policies. Based on the EU experience, a key vector for further development should be the harmonization of standards, enhancement of information environment transparency, and the establishment of a unified digital risk management system.

The institutional and legal integration of Ukraine into the European digital space is being carried out based on the Ukraine-EU Association Agreement (Section VI: "Economic and Sectoral Cooperation"); the Roadmap for Ukraine's Integration into the EU Single Digital Market (2023); and the Cybersecurity Action Plan in the Context of European Integration (2024–2026).

Harmonization of cybersecurity standards with EU norms requires synchronization across three dimensions: regulatory, institutional (creation of an interagency cyber resilience council), and technical (implementation of European protocols ISO/IEC 27001 and ENISA Best Practices). The main directions for adapting European cyber resilience standards in Ukraine are outlined in Table 4.

Ukraine's integration into the EU digital market opens opportunities not only for technological development but also for enhancing the country's economic resilience in conditions of war and recovery.

Amid ongoing armed aggression, Ukraine faces hybrid threats where cyberattacks are used as a tool of economic pressure. According to the ENISA Threat Landscape 2024, over 65% of incidents recorded in the Ukrainian cyberspace exhibited APT activity targeting the energy, banking, and transport logistics sectors.

Researchers [12] emphasize that a state's economic security in the digital environment is determined not only by the number of repelled attacks but also by the system's speed of adaptation to new types of threats. In 2025, the structure of digital risks to Ukraine's economic security has become comprehensive, combining technological, financial, institutional, and social factors (Table 5).

Table 4

Main directions for adapting European cyber resilience standards in Ukraine

Direction	European Analog	Ukrainian Equivalent	Implementation Status
Legislative framework	NIS2 Directive (2022)	Draft Law "On Cyber Resilience" (2025)	Under approval by the Cabinet of Ministers
Personal data	GDPR (2018)	Law "On Personal Data Protection"	Partial harmonization
Critical infrastructure	EU Cyber Resilience Act (2023)	Infrastructure Protection Strategy until 2030	Standards development
Incident monitoring	ENISA Threat Landscape	CERT-UA Reports	Implementation of analytical dashboards
Cyber education and workforce development	European Cybersecurity Academy	CyberSchool UA, Ministry of Digital Transformation	Pilot programs in 2024–2025

Source: compiled based on data from [2, 8]

Table 5

Key Digital Challenges for Ukraine's Economic Security in 2025

Risk Category	Manifestation	Potential Consequences for Economic Security	Mitigation / Neutralization Mechanisms	European Benchmark (Country / Initiative)
1	2	3	4	5
Energy	Cyberattacks on energy network management systems, SCADA systems, energy trading	Destabilization of the energy market, supply disruptions, economic losses	Implementation of ENTSO-E cybersecurity standards, use of SmartGrid Security Framework	Poland – Cyber Shield Energy Program
Financial	Breaches of payment platforms, manipulation of financial data, crypto asset fraud	Reduced trust in financial institutions, investor losses	Implementation of DORA, deployment of transaction monitoring systems	France – Banque de France Cyber Resilience Protocol
Information & Communication	Mass disinformation campaigns, phishing attacks, social engineering	Manipulation of public opinion, reduced political stability	Media literacy programs, AI-based content monitoring, population cyber hygiene	Estonia – Digital Society Trust Index

End of Table 5

1	2	3	4	5
Transport & Logistics	Cyberattacks on navigation systems, disruption of digital supply chains	Disruption of military and humanitarian logistics, increased costs	Use of cloud-based data recovery systems, GPS channel redundancy	Netherlands – Port Cyber Resilience Alliance
Industrial & Technological	Attacks on production networks, industrial data theft, shutdown of automated lines	Reduced production capacity, loss of competitiveness	Industrial system cybersecurity certification, critical asset audits	Germany – Industry 4.0 Security Roadmap
Education & Workforce	Shortage of cybersecurity specialists, low digital literacy of personnel	Insufficient threat response capacity	Development of CyberSchool UA programs, integration of STEM education, expert certification	Finland – National Cyber Education Framework
Institutional & Governance	Lack of a unified risk management system, limited interagency coordination	Delayed response, function duplication, increased systemic risks	Establishment of Cyber Resilience Council at the Cabinet of Ministers, integration of CERT-UA analytics	Lithuania – National Cyber Coordination Council

Source: compiled based on data from [2, 9–10]

The most critical segments remain the energy and financial sectors, which directly affect the resilience of the macroeconomic environment. At the same time, digital challenges in education and governance pose a long-term threat to the development of cybersecurity human capital.

Comparative analysis shows that the implementation of European practices (NIS2, DORA, Cyber Solidarity Act) reduces systemic risks and lays the groundwork for creating a national model of a cyber-resilient economy.

Based on data from ENISA (2022–2025), Eurostat, CERT-UA, and reports from the Ministry of Digital Transformation of Ukraine, a comparative assessment of key cybersecurity and digital maturity indicators was conducted (Table 6).

The analysis demonstrates a synchronized growth in Ukraine's cyber resilience and digital economy maturity from 2022 to 2025. The number of cyberattacks decreased by nearly 40%, while investment in digital security more than doubled. This positive trend is explained not only by technological factors but also by institutional strengthening of state governance, participation in European initiatives, and human capital development.

The increase in the digital maturity index to 0,74 in 2025 indicates a shift from an adaptive threat-response model to a predictive-analytical cyber resilience paradigm, consistent with EU practices.

It can therefore be concluded that the European experience in strengthening economic security through cyber resilience is highly relevant for Ukraine in the context of wartime and post-war challenges. Key research findings include:

The EU's cyber resilience institutional architecture is based on a multi-level responsibility model, integrating state governance, the corporate sector, and civil society.

Ukraine is gradually integrating European standards (NIS2, GDPR, DORA), but accelerated harmonization of technical standards and human resource capacity is needed.

The main drivers of cyber resilience are enhanced digital literacy, development of public-private partnerships, strengthening of analytical centers, and threat forecasting systems.

Implementing a national cyber resilience strategy aligned with ENISA principles and the Cyber Resilience Act will strengthen economic security, minimize digital risks, and ensure technological autonomy. Ukraine's cyber readiness level demonstrates positive convergence toward EU benchmarks (average 0,81).

Thus, cyber resilience is not merely a technical concept but a strategic foundation for sustainable economic development, governance, and international cooperation.

Conclusions. The study confirms that cyber resilience is a strategic prerequisite for strengthening economic security and technological autonomy. The European model – based on a combination of directive-based regulation (NIS2, DORA, GDPR), institutional cooperation (ENISA, CERT-EU), investment in human capital, and development of digital competencies – ensures stability of economic processes under crisis conditions. Ukraine shows positive convergence with the EU but requires further enhancement of human resources, increased funding, and the

Table 6

Trends in key cybersecurity and digital maturity indicators, 2022–2025

Indicator	2022	2023	2024	2025	Change Trend, %	Analytical Commentary
Ukraine Cyber Resilience Index	0,52	0,60	0,64	0,68	+30,8	Steady growth due to the launch of the National Cyber Incident Response Center (CERT-UA) and implementation of an early warning system
EU Cyber Resilience Index (average)	0,73	0,76	0,79	0,81	+11,0	Strengthening of analytical and coordination mechanisms within ENISA, Joint Cyber Unit, and Horizon Europe programs
Share of GDP allocated to cybersecurity, %	0,25	0,29	0,33	0,38	+52,0	Growth of budgetary and grant programs; Ukraine's participation in Digital Europe and EU4Digital
Number of recorded cyberattacks, thousand cases	156	132	118	96	−38,5	Decrease in attack frequency due to enhanced coordination with CERT-EU and expanded use of AI technologies for threat detection
Level of digital competencies of the population, %	55	58	60	62	+12,7	Positive dynamics resulting from the implementation of "Diia.Digital Education" and CyberSchool UA programs
Number of certified cybersecurity specialists	7,200	9,600	11,800	14,300	+98,6	Development of a qualified workforce, growth of private academies and state training programs
Share of enterprises with information security policies, %	41	48	54	61	+48,8	Activation of corporate security policies amid business digitalization and participation in international supply chains
Digital Economy Maturity Index (overall)	0,61	0,65	0,69	0,74	+21,3	Gradual transition from a fragmented to an integrated model of digital development in the public and private sectors

Source: compiled based on data from [2, 8–9]

establishment of an interagency Cyber Resilience Council. Implementing a national strategy based on the principles of the Cyber Resilience Act will minimize digital risks, strengthen macroeconomic stability, and increase Ukraine's integration into the EU Single Digital Market.

References

1. Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. *Applied Sciences*, 14 (24), 11807. DOI: https://doi.org/10.3390/app142411807
2. ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu
3. Haas, T. C. (2023). Adapting cybersecurity practice to reduce wildlife cybercrime. *Journal of Cybersecurity*, 9 (1), tyad004. DOI: https://doi.org/10.1093/cybsec/tyad004
4. Eurostat. (2025). *Digital economy and society statistics*. Available at: https://ec.europa.eu/eurostat/web/digital-economy-and-society/database
5. 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*, 14 (12), 2465. DOI: https://doi.org/10.3390/electronics14122465
6. CERT-UA. (2025). *Annual Report 2024–2025*. State Service of Special Communications of Ukraine. Available at: https://cert.gov.ua
7. Ristvej, J., Tonhauser, M., Chovanec, D., et al. (2025). Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports*, 15, 26902. DOI: https://doi.org/10.1038/s41598-025-12829-3
8. 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
9. Ministry of Digital Transformation of Ukraine. (2025). *Annual report on digital resilience and cybersecurity*. Available at: https://thedigital.gov.ua
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, 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

Бібліографічний список

1. Aghazadeh Ardebili A., Lezzi M., Pourmadadkar M. Risk assessment for cyber resilience of critical infrastructures: methods, governance, and standards. *Applied Sciences*. 2024. Vol. 14, No. 24. P. 11807. DOI: https://doi.org/10.3390/app142411807
2. ENISA Threat Landscape 2024. *European Union Agency for Cybersecurity*. URL: https://www.enisa.europa.eu
3. 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
4. Eurostat (2025). *Digital Economy and Society Statistics*. URL: https://ec.europa.eu/eurostat/web/digital-economy-and-society/database
5. 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
6. CERT-UA Annual Report (2024–2025). *State Service of Special Communications of Ukraine*. URL: https://cert.gov.ua
7. 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
8. 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
9. Ministry of Digital Transformation of Ukraine (2025). *Annual Report on Digital Resilience and Cybersecurity*. URL: https://thedigital.gov.ua
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

Буряк А.А.
кандидат економічних наук, доцент,
доцент кафедри міжнародних економічних відносин та туризму,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0002-0814-7459

Маслій О.А.
кандидат економічних наук, доцент,
доцент кафедри фінансів, банківського бізнесу та оподаткування,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0003-2184-968X

ЄВРОПЕЙСЬКИЙ ДОСВІД ЗМІЦНЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ НА ЗАСАДАХ КІБЕРСТІЙКОСТІ

У статті обґрунтовано теоретико-методологічні засади зміцнення економічної безпеки держави на основі розвитку кіберстійкості в умовах масштабної цифрової трансформації та зростання гібридних загроз. Розкрито зміст концепції кіберстійкості як багаторівневої системи запобігання, адаптації та відновлення після кіберінцидентів, що забезпечує стабільність функціонування фінансових, енергетичних, промислових і комунікаційних секторів. Узагальнено європейський досвід упровадження нормативно-правових актів NIS2, DORA, GDPR і Cyber

Resilience Act, які формують основу інтегрованої архітектури управління цифровими ризиками в ЄС. Визначено ключові структурні напрями забезпечення кіберстійкості – нормативно-правовий, інституційний, фінансово-інвестиційний, освітньо-комунікаційний, синергія яких забезпечує стійкість цифрової економіки та мінімізацію негативного впливу кіберзагроз на національний розвиток. Проведено порівняльний аналіз систем кіберстійкості ЄС і України, що виявив інституційну та ресурсну асиметрію, але водночас підтвердив динамічний прогрес України у гармонізації стандартів і зближенні показників цифрової зрілості. Доведено, що вітчизняна система кіберстійкості перебуває на етапі становлення, проте демонструє позитивну динаміку щодо впровадження європейських підходів, розвитку людського капіталу та зростання фінансування кіберзахисту. Зазначено, що формування національної системи кіберстійкості є стратегічним чинником підвищення макроекономічної стабільності, інвестиційної привабливості, технологічної самодостатності та інтеграції України до Єдиного цифрового ринку ЄС. Наукова новизна роботи полягає у розробленні концептуальної моделі зміцнення економічної безпеки держави на засадах інтеграції європейських практик кіберстійкості у національне цифрове врядування. Практична значущість результатів полягає у формуванні пропозицій щодо гармонізації законодавства України з нормами ЄС, створення міжвідомчої ради з питань кіберстійкості, розвитку публічно-приватного партнерства, цифрової освіти та підвищення культури кібербезпеки. Реалізація цих напрямів дозволить мінімізувати цифрові ризики, забезпечити безперервність економічних процесів, посилити довіру до цифрових інституцій та підвищити загальну стійкість національної економіки у воєнний і повоєнний періоди.

Ключові слова: економічна безпека, кіберстійкість, інформаційна безпека, безпекоорієнтоване інформаційне середовище, цифрові ризики.

Стаття надійшла: 15.09.2025
Стаття прийнята: 06.10.2025
Стаття опублікована: 31.10.2025