UDC 336.7:004.056:339.923(477)
JEL E61, F36
DOI 10.32782/2617-5940.2.2025.8

Olena Novytska
Candidate of Economic Sciences, Associate Professor,
State Tax University
ORCID: https://orcid.org/0000-0001-6451-7808
E-mail: novytska.ov@gmail.com

Valentyna Bykhovchenko
Candidate of Economic Sciences, Associate Professor
ORCID: https://orcid.org/0000-0002-7225-4646
E-mail: Color@gmail.com

Olena Alekhina
Second-Level Higher Education Applicant
(Master's Degree Applicant),
State Tax University
ORCID: https://orcid.org/0009-0004-7459-6780
E-mail: aliohinaolena@ukr.net

Anastasia Petrenko
Second-Level Higher Education Applicant
(Master's Degree Applicant),
State Tax University
ORCID: https://orcid.org/0009-0001-7687-9598
E-mail: petrenkonastya7@gmail.com

ADAPTATION OF THE EUROPEAN MODEL OF CYBERSECURITY FUNDING IN UKRAINE

Abstract. *The article is devoted to the analysis and improvement of mechanisms for adapting the European model of cybersecurity financing in Ukraine as a tool for accelerating economic convergence with the European Union. It is shown that full-scale war has radically increased the importance of cyber resilience as a component of national and economic security. It has been established that the increase in the frequency and complexity of cyberattacks requires not only technological but, above all, financial and economic solutions. Key market failures have been identified – insufficient investment, information asymmetry, and "war risk exclusion" – which limit the market's ability to provide an optimal level of cyber protection. It has been substantiated that effective counteraction to these failures is only possible through a combination of EU regulatory standards (NIS2 Directive) and targeted financial incentives. A model for adapting European cyber financing practices is proposed, with a focus on creating a National Cyber Financial Fund (NCF) as a state reinsurer of catastrophic risks and introducing a system of fiscal incentives for investments in NIS2 compliance. It has been proven that the formation of mixed financing mechanisms (public-private and donor) will ensure the sustainability of investments in cybersecurity and send a positive signal to international investors. The study uses methods of qualitative policy analysis, comparative modeling, and structural-functional synthesis. The results of the study confirm that the adaptation of EU financial instruments in the field of cybersecurity contributes to increasing Ukraine's investment attractiveness, developing the digital economy, and integrating into European value chains.*

Keywords: *cybersecurity, cyber resilience, NIS2, public-private partnership, cyber insurance, war risk, fiscal incentives, economic convergence, digital economy, EBRD.*

Олена Новицька
кандидат економічних наук,
Державний податковий університет
ORCID: https://orcid.org/0000-0001-6451-7808
E-mail: novytska.ov@gmail.com

Валентина Биховченко
кандидат економічних наук, доцент,
ORCID: https://orcid.org/0000-0002-7225-4646
E-mail: Color@gmail.com

Олена Альохіна
здобувачка вищої освіти другого (магістерського) рівня,
Державний податковий університет
ORCID: https://orcid.org/0009-0004-7459-6780
E-mail: aliohinaolena@ukr.net

Анастасія Петренко
здобувачка вищої освіти другого (магістерського) рівня,
Державний податковий університет
ORCID: https://orcid.org/0009-0001-7687-9598
E-mail: petrenkonastya7@gmail.com

АДАПТАЦІЯ ЄВРОПЕЙСЬКОЇ МОДЕЛІ ФІНАНСУВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Анотація. *Стаття присвячена аналізу та вдосконаленню механізмів адаптації європейської моделі фінансування кібербезпеки в Україні як інструменту прискорення економічної конвергенції з Європейським Союзом. Показано, що повномасштабна війна радикально підвищила значення кіберстійкості як складової національної та економічної безпеки. Установлено, що зростання частоти та складності кібератак вимагає не лише технологічних, а насамперед фінансово-економічних рішень. Визначено ключові ринкові провали – недостатнє інвестування, асиметрію інформації та «виключення воєнного ризику» – які обмежують здатність ринку забезпечувати оптимальний рівень кіберзахисту. Обґрунтовано, що ефективна протидія цим провалам можлива лише через поєднання регуляторних стандартів ЄС (Директива NIS2) та цільових фінансових стимулів. Запропоновано модель адаптації європейських практик кіберфінансування із фокусом на створенні Національного кібер-фінансового фонду (НКФФ) як державного перестраховика катастрофічних ризиків і запровадженні системи фіскальних пільг для інвестицій у NIS2-комплаєнс. Доведено, що формування змішаних механізмів фінансування (державно-приватних і донорських) забезпечить сталість інвестицій у кібербезпеку та створить позитивний сигнал для міжнародних інвесторів. У роботі використано методи якісного аналізу політики, порівняльного моделювання та структурно-функціонального синтезу. Результати дослідження підтверджують, що адаптація фінансових інструментів ЄС у сфері кібербезпеки сприяє підвищенню інвестиційної привабливості України, розвитку цифрової економіки та інтеграції у європейські ланцюги доданої вартості.*

Ключові слова: *кібербезпека, кіберстійкість, NIS2, державно-приватне партнерство, кіберстрахування, воєнний ризик, фіскальні стимули, економічна конвергенція, цифрова економіка, ЄБРР.*

Introduction. Economic recovery and accelerated convergence of Ukraine with the European Union (EU) require not only the restoration of physical infrastructure, but also the development of a highly resilient and reliable digital environment. In the context of full-scale military aggression, the number and complexity of cyber incidents in Ukraine increased by almost 70% in 2024. The use of artificial intelligence and "invisible" infiltration methods has been recorded [1]. This unprecedented level of cyber threats objectively shifts cybersecurity from the category of IT expenses to the category of critical national and economic stability.

Cyber resilience is defined as the ability of a system to resist cyber attacks and quickly recover, restoring system functionality [2]. This indicator is a key determinant of reliability for international investors who view Ukraine as part of global digital supply chains. Ensuring a high level of cyber resilience for critical infrastructure, in particular through the adoption and financial incentivization of EU standards, is a key element of economic policy.

The targeted adaptation of the European model of public-private cybersecurity financing, which includes cyber insurance mechanisms and tax incentives for private sector investment in accordance with the NIS2 Directive [3], will significantly accelerate Ukraine's economic convergence with the EU. This effect is achieved by ensuring the necessary level of confidence among international investors in the security of critical and digital infrastructure, which is a prerequisite for integration into global digital supply chains. However, despite institutional progress in the field of security, there are economic constraints.

Therefore, the effectiveness of digital environment protection is limited by classic market failures. An overview of these failures is critical to justify the need for public funding. Market mechanisms are not self-sufficient to ensure an optimal level of cybersecurity. International organizations, in particular the OECD, confirm that private sector firms tend to underinvest in this area because market forces are insufficient to adequately cover threats [4]. This phenomenon is explained by three main economic failures that require government intervention:

– underinvestment: security has a significant public good component. The benefits of one company's investment (e.g., in preventing the spread of malware) extend to the entire sector, reducing incentives for private capital to invest adequately [4];

– information asymmetry failure: the lack of unified, independently verified cybersecurity standards creates an information gap between international investors and investment targets. The NIS2 Directive serves as a quality signaling standard, providing investors with a universal marker of maturity and reliability [5];

– The War Exclusion Gap: it is critical for Ukraine that the commercial cyber insurance market does not cover critical incidents, as standard policies contain exclusions related to war (War Exclusion) and state cyberattacks [3]. The lack of adequate financial security makes it impossible to transfer (hedge) catastrophic risk. As a result, there is an urgent need for direct subsidies or guarantees from state or international institutions.

Literary review. Since market mechanisms cannot correct these failures on their own, targeted government intervention is necessary. Therefore, regulatory requirements (NIS2) generate the need for investment, while financial incentives (tax breaks) and risk sharing (cyber insurance/reinsurance) make these investments economically attractive. Research on the relationship between cybersecurity and economic integration is based on a critical analysis of international scientific publications and official documents. Scientists [2] and international organizations, such as the OECD, confirm the existence of market failures in the field of cybersecurity, which lead to insufficient levels of private investment.

Regulatory policy plays a central role in correcting these shortcomings. Directive NIS2 (Directive (EU) 2022/2555) [3] is decisive because it transforms security

costs into a measurable value of protection [6], increasing operational resilience. Regulatory harmonization acts as a quality signal for global trade and foreign direct investment (FDI), removing non-tariff barriers and increasing trust [7]. Failure to comply with international standards can be interpreted as discrimination or a violation of fair and equitable treatment (FET) standards for foreign investors, creating risks in investment arbitration [8].

As stated in the NIS2 Directive, the biggest challenge for Ukraine is the "war exclusion gap." Since standard cyber insurance policies contain war-related exclusions [3], this creates a financial vacuum. The solution is state intervention in the form of creating reinsurance mechanisms [9], implementing a successful model that has already been implemented for physical military risks with the support of the European Bank for Reconstruction and Development (EBRD) [10]. Thus, scientific literature and international policy agree that only the integration of regulatory requirements (NIS2) with targeted financial instruments (tax incentives and risk sharing) can mobilize private capital to ensure the necessary level of cyber resilience.

Methodology. The study is based on policy analysis and the application of a structural-functional approach with elements of quantitative modeling.

The main part. The NIS2 Directive (Directive (EU) 2022/2555) is a fundamental regulatory act that establishes a common cybersecurity standard within the European Union. It covers 18 critical sectors of the economy and public life (from energy and finance to the production of critical goods and waste management), establishing a unified approach to cyber risk management for "essential" and "important" organizations [11].

For international investors, Ukraine's adoption of NIS2 means that critical infrastructure facilities operate under the same proven security standards applied in the EU. This objectively reduces the uncertainty associated with cyber risk and turns regulatory harmonization into a powerful factor in investment attractiveness [7].

Strengthening risk management requirements in general directly leads to the need to focus on the most vulnerable elements of modern digital systems. With this in mind, NIS2 pays critical attention to supply chain protection. One of the most far-reaching requirements of NIS2 is the mandate to strengthen supply chain security [7]. Organizations are becoming increasingly dependent on external suppliers, and supply chains have become a vulnerable link in cybersecurity.

For Ukrainian companies seeking to integrate into European digital supply chains, NIS2 compliance is becoming a mandatory condition for admission. European organizations are required to verify the cyber maturity of their external partners. Companies that do not comply with NIS2 requirements risk losing their competitive advantage [12]. NIS2 tightens security requirements for suppliers [7], which is a direct mechanism for removing non-tariff barriers to trade and accelerating economic convergence.

Supply chain security requirements are a prerequisite for trade, but the NIS2 regulatory framework also contains powerful enforcement mechanisms that transform investment behavior. Therefore, NIS2 introduces enhanced oversight and enforcement mechanisms, including the possibility of imposing substantial financial penalties, calculated on the basis of a company's global turnover, for non-compliance [13]. These fines, as well as the inevitable reputational damage resulting from a cyber incident, can deal a critical blow to financial stability [12].

This regulatory pressure is forcing organizations to rethink their cybersecurity spending. It is transforming from a regulatory burden to an investment in operational resilience and business continuity (Business Continuity Investment Framework) [6]. NIS2 requires management to take direct responsibility for approving and implementing cybersecurity strategies [14]. Thus, NIS2 effectively transforms compliance costs into measurable protection value, as both the likelihood of an incident and its potential impact are reduced [6].

The regulatory pressure of NIS2, exacerbated by the threat of significant sanctions, generates the necessary demand for cyber protection. However, EU member states are actively using financial mechanisms to correct market failures associated with insufficient investment. That is why these instruments need to be purposefully adapted in Ukraine to finance NIS2 compliance.

OECD studies show that tax policy is crucial for stimulating private investment. Although high corporate tax rates can have a negative impact on investment, tax incentives for research and development have a proven positive effect on productivity [15]. A similar targeted approach is needed for cybersecurity.

European countries are already considering similar mechanisms. For example, Germany is discussing the possibility of exempting investments in IT security from the debt brake, recognizing cybersecurity as a strategic investment priority [16].

To accelerate convergence, Ukraine needs targeted fiscal incentives directly linked to investments in NIS2 compliance. These could include:

– tax credit for investments. Provide a direct percentage of the cost of NIS2-compliant equipment and certification;

– accelerated depreciation deductions. Allow entities covered by NIS2 to quickly write off capital expenditures on cybersecurity. This mechanism reduces the user cost of capital and encourages companies to upgrade their systems immediately [15].

Fiscal instruments provide direct investment incentives, but they do not solve the problem of risk distribution. Therefore, an additional mechanism is needed to act as a financial lever and maturity stimulator. This is precisely the role played by cyber insurance, which is a key risk transfer tool. Companies that can demonstrate a high level of compliance (for example, by implementing the measures required by NIS2) can expect lower insurance premiums [6]. This creates a measurable financial ROI for NIS2 compliance.

Insurers often act as de facto regulators of cyber maturity. To obtain coverage, they require customers to implement certain controls (e.g., multi-factor authentication). These requirements serve as a powerful lever for organizations that are forced to invest in order to meet underwriting requirements. Insurance requirements can be useful levers for promoting cybersecurity funding by overcoming institutional barriers [14].

Adapting successful European regulatory and financial models requires taking into account the unique risks of wartime. Despite overall progress in harmonization, a targeted financial shield is needed to address critical market

failure. Therefore, a targeted public-private partnership model is needed.

Ukraine is showing significant progress in harmonizing legislation, which is a signal to international partners. The adoption of the Law of Ukraine "On Amendments to Certain Laws of Ukraine on Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure" [17] laid the foundation for a new national cybersecurity framework, consistent with the conditions for receiving funding from the Ukraine Facility [18]. Institutional integration is confirmed by Ukraine's access to the EU Cybersecurity Reserve in July 2025, which provides operational assistance in the event of large-scale cyberattacks [1].

Existing models of public-private cooperation (PPP) in Ukraine, such as the National Cyber Cluster, MISP-UA, and CERT-UA, effectively facilitate the exchange of information about incidents and joint research and development [19]. However, these models are insufficient to mobilize the large amount of private financial capital required for large-scale NIS2 compliance of critical infrastructure.

Despite significant progress in developing the institutional framework and harmonizing legislation, there is a critical gap in financial risk coverage. The biggest obstacle to the implementation of a public-private cybersecurity financing model in Ukraine remains the high military risk, which is excluded by international private insurers through the "War Exclusion" clause [3].

The European Bank for Reconstruction and Development (EBRD) has already successfully developed and implemented reinsurance mechanisms that enable local Ukrainian insurance companies to offer policies covering military risks. This partnership with international financial institutions and donors allows for the effective distribution of catastrophic risks, exceeding the capital limits of national insurers [10].

It is also advisable to adapt this EBRD model to cover cyber risks associated with military operations. To this end, it is proposed to establish a National Cyber Financial Fund (NCF), which will act as a state reinsurer of "catastrophic" cyber risks caused by war. It would be advisable to provide financial support for the Fund through donor contributions, in particular through the use of resources and instruments provided by the Tallinn Mechanism [20] or similar international platforms. This would allow:

– minimize financial losses of critical infrastructure entities from large-scale cyberattacks;

– ensure the liquidity of the insurance market, which is unable to cover wartime risks on its own;

– encourage Ukrainian companies to implement high cybersecurity standards through the availability of insurance products.

In our opinion, this approach guarantees the stability of critical digital systems even in conditions of heightened military threat. Risk sharing will allow private insurers to resume providing commercial cyber insurance for "normal" cyber incidents.

Overcoming the cyber insurance crisis and eliminating the War Exclusion Gap also requires the creation of an innovative financial architecture. With this in mind, the proposed NIS2 compliance financing architecture should combine state guarantees, international blended financing, and targeted fiscal incentives:

1. DFI instruments. Involvement of blended finance mechanisms from the International Finance Corporation (IFC) and the EBRD. These institutions can provide financial guarantees and assume increased risk for critical infrastructure projects, but with the clear condition that these projects achieve NIS2 compliance [21].

2. Adaptation of InvestEU. Use of European investment platforms such as InvestEU, which are aimed at supporting innovation [22]. Similar mechanisms should be adapted to support Ukrainian high-tech companies developing NIS2-compliant solutions.

The implementation of a comprehensive architecture for financing NIS2 compliance goes beyond purely technical requirements, constituting a strategic tool for influencing key macroeconomic indicators. Accordingly, it is advisable to consider the correlation between cyber resilience and the investment attractiveness of the national economy.

Investments in cybersecurity are recognized as a critical element of national and economic security [21]. The increase in the intensity of attacks on critical infrastructure directly correlates with an increase in risk perception by international investors [8].

The adoption of the NIS2 Directive and the creation of a stable cyber risk financing mechanism send a powerful signal of quality. Harmonized international standards, such as NIS2, increase trust and facilitate international trade and foreign direct investment (FDI) [7].

Compliance by critical infrastructure entities in Ukraine with the same risk management requirements as in the European Union removes significant regulatory and operational barriers for foreign investors. Conversely, Ukraine's failure to meet these standards could be interpreted as discrimination or a violation of fair and equitable treatment (FET) standards towards investors, which in turn creates risks in the context of investment arbitration [8]. Thus, the cyber resilience provided by NIS2 is a fundamental condition for attracting international capital.

In addition to its direct impact on FDI, cyber resilience critically affects the economy's ability to integrate into international trade structures. Integration into European digital supply chains is a direct path to economic convergence.

The NIS2 Directive tightens security requirements for suppliers [7], requiring suppliers from third countries, including Ukraine, to comply with similarly high standards. Achieving NIS2 compliance by Ukrainian suppliers significantly reduces barriers to their participation in European trade. This not only increases export potential but also contributes to deeper structural integration of the economy, as Ukrainian companies are positioned as reliable links in global digital ecosystems.

The growth in export potential and the removal of trade barriers caused by NIS2 compliance generate a cumulative effect that positively affects overall economic development. Therefore, a high level of cyber resilience and a reliable digital infrastructure are recognized as fundamental factors for long-term economic growth and stability [21].

The creation of an effective financial mechanism for cybersecurity will enable Ukraine to significantly increase investment in this area. For comparison, total cybersecurity spending in the United States is about 0.35% of GDP [22]. If Ukraine can mobilize private capital through NIS2 incentives and a risk-sharing mechanism, this will

ensure the necessary level of investment, accelerating structural alignment with European economic models.

To systematize the proposed NIS2 compliance financing instruments and their role in correcting market failures necessary for economic convergence, Table 1 presents an analysis of the key financial mechanisms used in the EU and their targeted adaptation to the Ukrainian context.

The creation of the NCF addresses the issue of catastrophic risk, but additional incentives are needed to ensure the necessary level of sufficient private sector investment. Thus, to overcome the trend of underinvestment in cybersecurity, targeted fiscal incentives directly linked to NIS2 compliance costs need to be introduced:

– accelerated depreciation deductions. Allow NIS2-covered companies to accelerate the depreciation of capital expenditures on security equipment. This encourages immediate investment by reducing the opportunity cost of capital [15];

– investment tax credit. Provide a tax credit for expenses related to the audit and certification required to comply with NIS2.

The effectiveness of the above policy interventions requires the creation of a monitoring system to assess their impact on macroeconomic convergence. To this end, Table 2 presents key convergence indicators that allow measuring the success of the proposed solutions.

Conclusions. The systematic implementation of targeted financial adaptation of the European cybersecurity model in Ukraine, with an emphasis on achieving compliance with the requirements of the NIS2 Directive (on high common cybersecurity measures in the EU), is an imperative prerequisite for accelerating economic convergence with the European Union, as the cyber resilience of critical infrastructures is crucial for integration into the EU internal market. Based on the identified critical role of financial adaptation of cybersecurity and NIS2 compliance, there is an objective need to develop, validate, and further implement specific organizational, technical, and financial measures that enable an effective transition from declarative to functional compatibility. Thus, the strategic recommendations for ensuring the implementation of the above-mentioned process are as follows:

– creation of the NCFF. It is necessary to urgently introduce a model of public-private risk sharing in the cyber sphere by creating a National Cyber Financial Fund (NCFF) to reinsure catastrophic cyber risks associated with war. Full NIS2 compliance should be a condition for access to this reinsurance.

– introduction of targeted fiscal incentives. To stimulate investment, targeted tax incentives should be introduced, including accelerated depreciation allowances and investment tax credits directly linked to NIS2 compliance costs.

– integration of DFI financing with NIS2. All critical infrastructure financing programs implemented by international financial institutions (EBRD, IFC) should include NIS2 compliance as a mandatory condition, using blended finance mechanisms to mitigate risk.

Table 1

Analysis of financial mechanisms for stimulating cyber investments and their adaptation for Ukraine

Incentive mechanism	Mechanism of action (economic correction)	EU examples	Proposed adaptation for Ukraine (link to NIS2)
Mandatory regulatory standards (NIS2)	correction of market failure due to insufficient investment; establishment of minimum quality/safety thresholds	NIS2 Directive	Legislative transposition of NIS2; linking compliance to licensing of critical services
Cyber insurance/	risk transfer, risk pricing;	Premium reductions for improved risk profiles	Creation of a National Cyber Financial Fund (NCF) to cover military cyber risks
reinsurance	leverage for the implementation of internal controls	IT security exempt from debt brakes (Germany)	Accelerated depreciation deductions and targeted investment tax credits (ITC) for NIS2 expenses
Fiscal incentives (tax breaks)	reduction of user cost of capital;	InvestEU	Attracting EBRD/IFC guarantees and blended finance for critical infrastructure cyber projects that have achieved NIS2 compliance

Source: [3, 6, 10, 11, 15-17, 21]

Table 2

Quantitative indicators of the impact of NIS2 on economic convergence

Sphere of influence	Key vector	Convergence indicator (Output Metric)	Source data (source)
Investment confidence (FDI)	NIS2 as a sign of quality and reduced systemic risk	Growth in FDI in critical infrastructure requiring NIS2 compliance; Reduction in risk premium for NIS2 sectors.	OECD Economic Surveys.
Financial stability of business	Cyber insurance reduces the financial impact of incidents	Ratio of reduction in insurance premiums for NIS2-compliant companies; Measurable ROI from NIS2 compliance.	ENISA reports.
Integration into supply chains	NIS2 compliance removes non-tariff barriers to trade	Number of Ukrainian suppliers certified to NIS2 standards; Growth in exports of digital services to the EU.	ENISA reports.
Public-private partnership	Effectiveness of the risk-sharing mechanism (NKFF)	Share of private capital mobilized under state/ international guarantees in critical infrastructure cyber projects.	DFI (EBRD/IFC) data, NCFF.

Source: [5–7, 10]

References:

1. SSSCIP of Ukraine. Cybersecurity: Market to hit $200m as attacks grow. (2024). Available at: https://itukraine.org.ua/en/ukraine-s-cybersecurity-market-to-hit-200m-as-attacks-grow-in-sophistication/ (accessed: 07.09.2025).

2. Weisman, Michael Kott, Alexander Ellis, Jason Murphy, Brian Parker, Travis Smith, Sidney Vandekerckhove, Joachim. (2023). Quantitative Measurement of Cyber Resilience: Modeling and Experimentation. 10.48550/arXiv.2303.16307. (2023). Available at: https://www.researchgate.net/publication/369623557_Quantitative_Measurement_of_Cyber_Resilience_Modeling_and_Experimentation (accessed: 07.09.2025).

3. The NIS2 Directive : European Commission. (2022). Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (accessed: 07.09.2025).

4. Building Stronger Defences for a Digital Future: The Role of Cybersecurity : OECD. (2025). Available at: https://www.oecd.org/en/publications/economic-security-in-a-changing-world_78f3b129/full-report/building-stronger-defences-for-a-digital-future-the-role-of-cybersecurity_484bcb90.html (accessed: 10.09.2025).

5. NIST. Risk Management and Security Metrics: Challenges and Policy Solutions. (2017). Available at: https://www.nist.gov/system/files/documents/2017/05/09/report13-1.pdf (accessed: 10.09.2025).

6. Acre Security. Understanding NIS2: Why Companies Must Prioritize Compliance. (2024). Available at: https://acresecurity.com/blog/understanding-nis2-why-companies-must-prioritize-compliance (accessed: 27.09.2025).

7. Kiteworks. NIS2 Compliance Costs vs. Financial Benefits. (2024). Available at: https://www.kiteworks.com/regulatory-compliance/nis2-compliance-costs/ (accessed: 07.10.2025).

8. How Do Taxes Affect Investment and Productivity? An Industry-Level Analysis of OECD Countries : OECD. (2015). Available at: https://www.oecd.org/en/publications/how-do-taxes-affect-investment-and-productivity_230022721067.html (accessed: 07.10.2025).

9. Telefonica Tech. NIS2 Directive (II): Cyber Security obligations and their impact on European businesses. (2024). Available at: https://telefonicatech.com/en/blog/nis2-directive-ii-how-cyber-security-obligations-affect-european-businesses (accessed: 07.10.2025).

10. IT security soon to be exempt from debt brake? : Daturex GmbH. (2025). Available at: https://externer-datenschutzbeauftragter-dresden.de/en/data-protection/it-security-soon-to-be-exempt-from-debt-brake/ (accessed: 17.09.2025).

11. Aon. Bridging the NIS2 Cyber Security Gap. (2024). Available at: https://www.aon.com/en/insights/articles/bridging-the-nis2-cyber-security-gap (accessed: 27.09.2025).

12. EBRD. First Ukrainian companies take advantage of new war risk insurance. (2025). Available at: https://www.ebrd.com/home/news-and-events/news/2025/first-ukrainian-companies-take-advantage-of-new-war-risk-insuran.html (accessed: 27.09.2025).

13. MFA of Ukraine. Norway Joins the Tallinn Mechanism to Support Ukraine's Cyber Resilience. (2025). Available at: https://mfa.gov.ua/en/news/norvegiya-priyednalasya-do-tallinnskogo-mehanizmu-pidtrimki-kiberstijkosti-ukrayini (accessed: 27.09.2025).

14. World Bank Group. Donor Financing Mechanisms for Supporting Ukraine. (2025). Available at: https://www.worldbank.org/en/country/ukraine/brief/world-bank-group-donor-financing-mechanisms-for-supporting-ukraine (accessed: 07.10.2025).

15. Educause. Frequently Asked Questions About Cyber Insurance. (2025). Available at: https://library.educause.edu/resources/2025/5/frequently-asked-questions-about-cyber-insurance (accessed: 07.10.2025).

16. Morgan Lewis. Update: Ukraine Conflict Has Implications for Cyberinsurance Policies, Including War Exclusions. (2022). Available at: https://www.morganlewis.com/pubs/2022/03/update-ukraine-conflict-has-implications-for-cyberinsurance-policies-including-war-exclusions (accessed: 07.10.2025).

17. On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Objects / Law of Ukraine No. 4336-IX of March 27, 2025. Available at: https://zakon.rada.gov.ua/laws/show/4336-20#Text (accessed: October 7, 2025).

18. The government approved the Plan for the implementation of the Ukraine Facility program: Ministry of Economy of Ukraine. Available at: https://www.kmu.gov.ua/news/uriad-zatverdyv-plan-dlia-realizatsii-prohramy-ukraine-facility (accessed: 07.10.2025).

19. ResearchGate. Current State of Public-Private Partnership in the Field of Cybersecurity: Ukrainian Experience. (2024). Available at: https://www.researchgate.net/publication/396022298_CURRENT_STATE_OF_PUBLIC-PRIVATE_PARTNERSHIP_IN_THE_FIELD_OF_CYBERSECURITY_UKRAINIAN_EXPERIENCE (accessed: 10.10.2025).

20. OUP/JIDS. Data privacy and cybersecurity regulations and their implications for foreign investors. (2024). Available at: https://academic.oup.com/jids/article/16/3/idaf020/8173308 (accessed: 10.10.2025).

21. Pinsent Masons. Insurance arrangements pivotal to Ukraine rebuild. (2023). Available at: https://www.pinsentmasons.com/out-law/analysis/insurance-arrangements-pivotal-ukraine-rebuild (accessed: 11.10.2025).

22. European Court of Auditors (ECA). EU Cybersecurity Spending. (2024). Available at: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf (accessed: 10.10.2025).

Стаття надійшла: 10.10.2025
Стаття прийнята: 26.10.2025
Стаття опублікована: 27.11.2025