The formation of a national strategy for cyber protection of critical infrastructure facilities

Oleksii Hutsaliuk[1,*,†], Iuliia Bondar[2,†], and Oksana Yakusheva[3,†]

[1] *Private Higher Education Institution «Rauf Ablyazov East European University», Nechuya-Levytskogo, 16, 18036, Cherkasy, Ukraine*

[2] *Volodymyr Vynnychenko Central Ukrainian State University, Shevchenka, 1, 25006, Kropyvnytskyi, Ukraine*

[3] *Cherkasy State Technological University, Shevchenka, 460, 18000, Cherkasy, Ukraine*

Abstract

The article substantiates the conceptual foundations for developing Ukraine's national cybersecurity strategy for critical infrastructure in the context of digitalization, hybrid threats, and escalating cyberattacks. The number of registered cyber incidents increased by 62.5% in 2023 and almost 70% in 2024, confirming the need for an integrated cyber risk management system. The proposed model provides a multi-level hierarchy including a national cybersecurity coordinator, sectoral authorities, critical infrastructure operators, a scientific council, and international partners. Ukraine faces a shortage of about 100,000 cybersecurity specialists, yet the market is growing dynamically – from $35 million in 2016 to $138 million in 2024, with projections of $209 million by 2029. The developed strategy aims to ensure the cyber resilience of critical sectors, align with the NIS2 Directive, strengthen public-private partnerships, and enhance international cooperation, reducing economic losses and increasing trust in state institutions. The formation of a national strategy for cyber protection of critical infrastructure is a key element of national security under digitalization and hybrid threats, combining risk-based management, legal frameworks, workforce development, and partnerships to enhance resilience and integrate Ukraine into the global cybersecurity system.

Keywords

cybersecurity, critical infrastructure, cyber resilience, risk-oriented management, public-private partnership, national economy.

1. Introduction

Critical infrastructure facilities (CIF) (energy, transport, banking and financial system, government IT resources) is increasingly exposed to cyberattacks in the condition of modern digital transformation of public administration and the economy. According to the State Service for Special Communications, in 2023 the number of recorded cyberattacks against state bodies of Ukraine increased by 64% compared to 2021, and in the energy sector – by 50%. The losses from cybercrime worldwide are estimated at over $8 trillion annually (Cybersecurity Ventures, 2023), which is about 9% of global GDP [1-2].

In the context of hybrid threats, it is critically important for Ukraine to form a holistic national cyber-protection strategy based on the principles of proactivity, risk-oriented regulation, and international coordination. Public-private partnership is an important factor, as about 80% of critical infrastructure facilities belong to the private sector.

Implementing a cyber-protection strategy should encompass not only technical and legal dimensions, but also human resources, educational programs, and integration into the global cybersecurity system. This will improve the state's resilience to cyber challenges and reduce potential losses, which, according to EU forecasts, could reach 1.5% of global GDP by 2030 in the absence of proper protection.

[1] *SMICS'25: Workshop on Cryptology and Data Security, October 16-18, 2025, Lviv, Ukraine*

*Corresponding author.

† These authors contributed equally.

alex-g.88@ukr.net (O. Hutsaliuk); cooperjulia@ukr.net (Iu. Bondar); o.yakusheva14@gmail.com (O. Yakusheva)

0000-0002-6541-4912 (O. Hutsaliuk); 0000-0003-2269-6208 (Iu. Bondar); 0000-0002-4849-0323 (O. Yakusheva)

The purpose of the paper is to substantiate the principles and tools of the national CIF cyber-protection strategy, which combines risk-oriented regulation, public-private interaction and readiness for incidents.

2. Results

In 2024–2025, the EU significantly updated the framework for cyber resilience of critical sectors through NIS2 and related implementing acts: ENISA summarizes the state of country capabilities and offers policy recommendations (Reviews of the State of Cybersecurity of the Union-2024, Technical Guides on the Implementation of NIS2 2025). This reinforces the requirements for risk management, incident reporting and oversight at Member State and sector level [3].

Ukraine relies on the Cybersecurity Strategy (Decree No. 447/2021) and the updated legal framework for the protection of critical infrastructure (Law No. 1882-IX with amendments in force until August 22, 2024). In parallel, state reports of the State Service for Special Communications and Information Protection (SSSCIP) record the evolution of threats and lessons learned from three years of cyber warfare, highlighting the need for interagency coordination, incident management, and international cooperation [4].

Practical guidelines for CIF operators are offered by ENISA (NIS2 implementation guidelines, sectorial threat landscapes) and CISA (CPGs as a baseline for IT/OT). These materials specify control measures, evidence of compliance, and mapping of requirements to standards, which is convenient to integrate into national policies and departmental regulations.

Current tasks include synchronizing sectorial regulation with NIS2/CER, building a national system of supervision, registration of entities and incident reporting processes, as well as developing the capabilities of competent authorities. Tracking the transposition of NIS2 shows the uneven progress of states and the importance of clear secondary acts and methodological materials. To date, 14 out of 27 EU Member States have implemented the NIS2 Directive into national legislation (Fig. 1) [5-6].

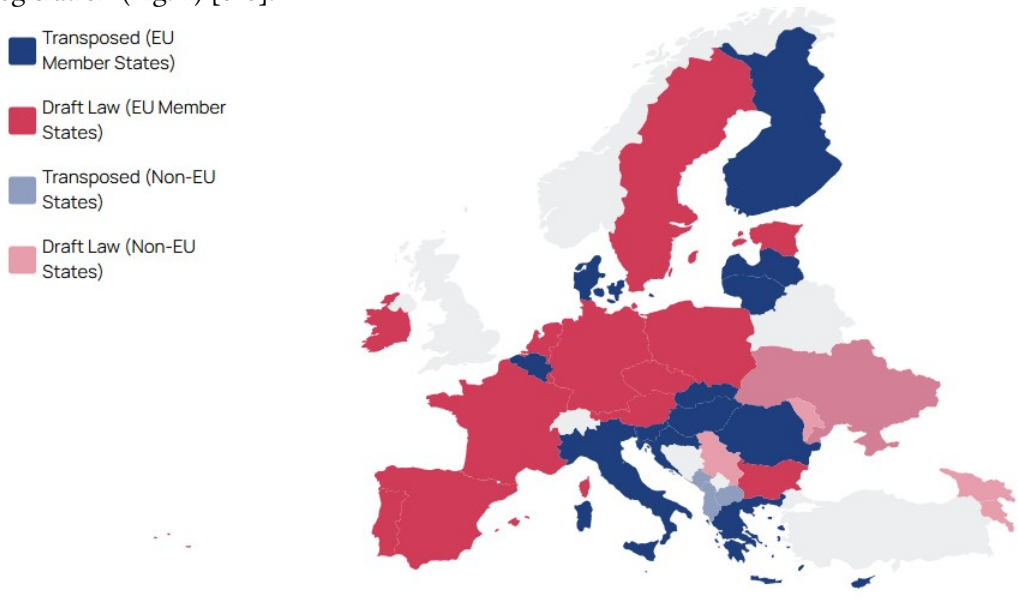

Figure 1: Implementation of the NIS2 Directive by EU Member States into national legislation (NIS2 Directive Transposition Tracker; NIS2 Technical Implementation)

The rapid digitalization of critical sectors – energy, transport, communications, finance, healthcare, public services, water supply and the defense-industrial complex – is accompanied by the escalation of hybrid threats. The changes come amid a sharp increase in cyber incidents:

2,543 cyberattacks were recorded in Ukraine in 2023 – 15.9% more than in 2022. Of these: 347 attacks on government agencies, 92 on energy, 81 on telecommunications, 32 on transport, 30 on finance, 12 on medicine [7]. In 2024, the number of attacks increased to 4,315 incidents - almost 70% more than the previous year [8]. Attackers are spreading malware, phishing, and account compromise; the target is energy, government, defense, and telecommunications.

At the same time, energy infrastructure is under massive physical and cyber attacks. Thus, in August 2024, about 8 million households were left without electricity as a result of airstrikes. About half of the electricity generation capacity (including 6 GW at the ZNPP) and half of the high-voltage substations were destroyed or damaged in 2022–2023. A massive missile and drone strike in March 2024 knocked out 80% of the power capacity of one of the private energy companies (DTEK), cutting off power supply to 1.9 million people [9].

In January 2024, the APT44/Sandworm cyber group attacked more than 20 energy, water, and heating facilities. For example, in Lviv, heating and hot water were turned off for over 600 homes during the frost.

In addition, there is a critical shortage of cybersecurity professionals. According to estimates from the State Special Communications Service, Ukraine may lack up to 100,000 such specialists. Despite this, the cybersecurity market in Ukraine is actively growing: in 8 years it has grown 4 times – to 138 million USD in 2024. The forecast is +50% over the next five years to $209 million [10].

The formation of a national strategy for cyber protection of critical infrastructure facilities should be based on clearly defined methodological foundations and principles. It should provide a comprehensive approach that integrates cyber, physical and information security into a single resilience management system. Risk-orientation is of particular importance, which involves prioritizing measures taking into account industry threat scenarios and the possible impact on the provision of socially important services. The strategy should be proactive and include security on default, which means establishing requirements for secure software development, architectures, networks, and supply chains at the design stage. An important condition is compatibility with global standards, in particular ISO/IEC 27001/2, 62443, NIST CSF and other cyber resilience standards for OT/ICS.

According to SSSCIP and CERT-UA, the number of cyberattacks in Ukraine in 2024 increased by almost 70% – to 4,315 incidents compared to 2,541 in 2023. The response system processed about 3 million information security events, of which 28,000 were critical, and analysts directly processed 1,042 cyber incidents in 2024 [11]. In 2023, 1,105 cyber incidents were recorded – 62.5% more than in 2022 [12]. The cybersecurity market in Ukraine grew to $138 million in 2024 and is projected to grow to $209 million within five years [13].

Within the framework of the National Cybersecurity Strategy for Critical Infrastructure, a clear organizational model of state governance is envisaged, defining the roles and responsibilities of key stakeholders. The model provides for the functioning of a central coordinating entity – the National Cybersecurity Coordinator or Cyber Center, responsible for strategic planning, policy development, sectoral CSIRT certification, and centralized data exchange on cyber threats. Across specific sectors – such as energy, transportation, and others – competent authorities carry out supervision, maintain an inventory of critical infrastructure objects, approve cybersecurity plans, and conduct compliance audits. The National CERT/CSIRT processes cyber incident reports, coordinates response actions, and disseminates alerts and early warnings.

Critical infrastructure operators are tasked with implementing protective measures, managing risks, reporting incidents, participating in training activities, and ensuring the continuity of essential services. The scientific and expert council is responsible for developing risk assessment methodologies, standardization, workforce training, and threat analysis. At the international level, partner organizations facilitate cyber intelligence sharing, joint exercises, and mutual assistance in the event of major incidents.

In addition, the governance model includes the creation of a dynamic registry of critical services, functions, and corresponding operators. This registry is formed based on criteria such as scale of impact, interdependencies, cross-border effects, irreplaceability, and level of digitalization. Such a model ensures management flexibility and timely updates of information on critical infrastructure assets.

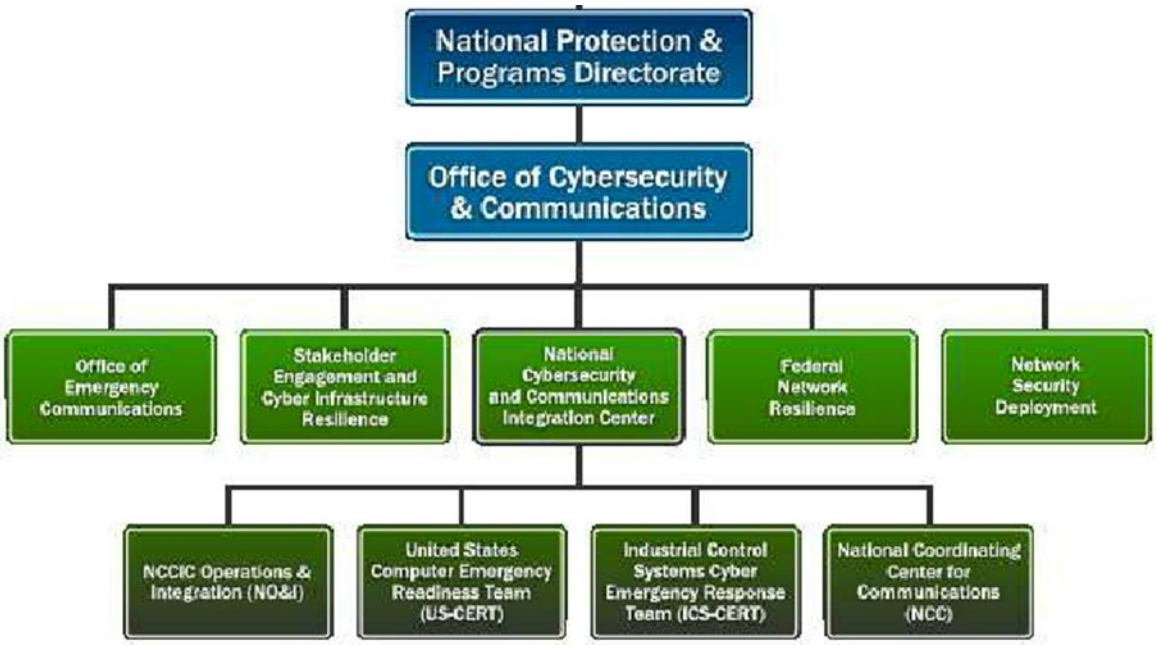

Figure: 2. Structural Model of the National Cybersecurity Center with Different Levels and Units

In Figure 2, the organizational structure is presented in a hierarchical form: at the top level is the national coordinating body/Cybersecurity Center, which directly interacts with the national CSIRT/CERT and competent sectoral authorities. In parallel, a scientific and expert council operates, providing methodological support, standardization, and training resources. At the sectoral level, critical infrastructure operators implement the practical application of cybersecurity measures. Finally, the entire structure is connected with external international partners, who provide intelligence sharing, training, and operational support.

Thus, the presented model of the National Cybersecurity Center reflects the organizational architecture of the cybersecurity management system at the state level. It demonstrates multilevel interaction between central security agencies, governmental structures, scientific and analytical units, CERT centers, and sectoral coordinators. Such a hierarchical configuration ensures coordination of actions among national entities responsible for detecting, preventing, and responding to cyber incidents and establishes a foundation for cooperation with international cybersecurity structures. The organizational interconnection between levels enables rapid information response, standardized data exchange, and efficient decision-making in crisis situations.

However, the effective functioning of this structure requires not only organizational coordination but also a strategic vision for risk management, the distribution of responsibilities, and the development of policies and standards for protecting critical information resources. Therefore, the next logical step is the formation of a national cybersecurity strategy for critical infrastructure, presented in Figure 3. This model summarizes approaches to creating an integrated system for countering cyber threats, combining technical, organizational, regulatory, and international components.

Figure 3 presents a hierarchical system: at the top level is the national risk management model, which integrates subsystems for monitoring, assessment standards, and incident classification. Below are sectoral subsystems responsible for risk assessment and response. At the level of critical infrastructure operators, architectural controls and functional support are implemented. All components are interconnected through information exchange channels and regular updates of risk models. External structures – analytics, testing, and backup systems – are integrated into the process of strategic improvement.

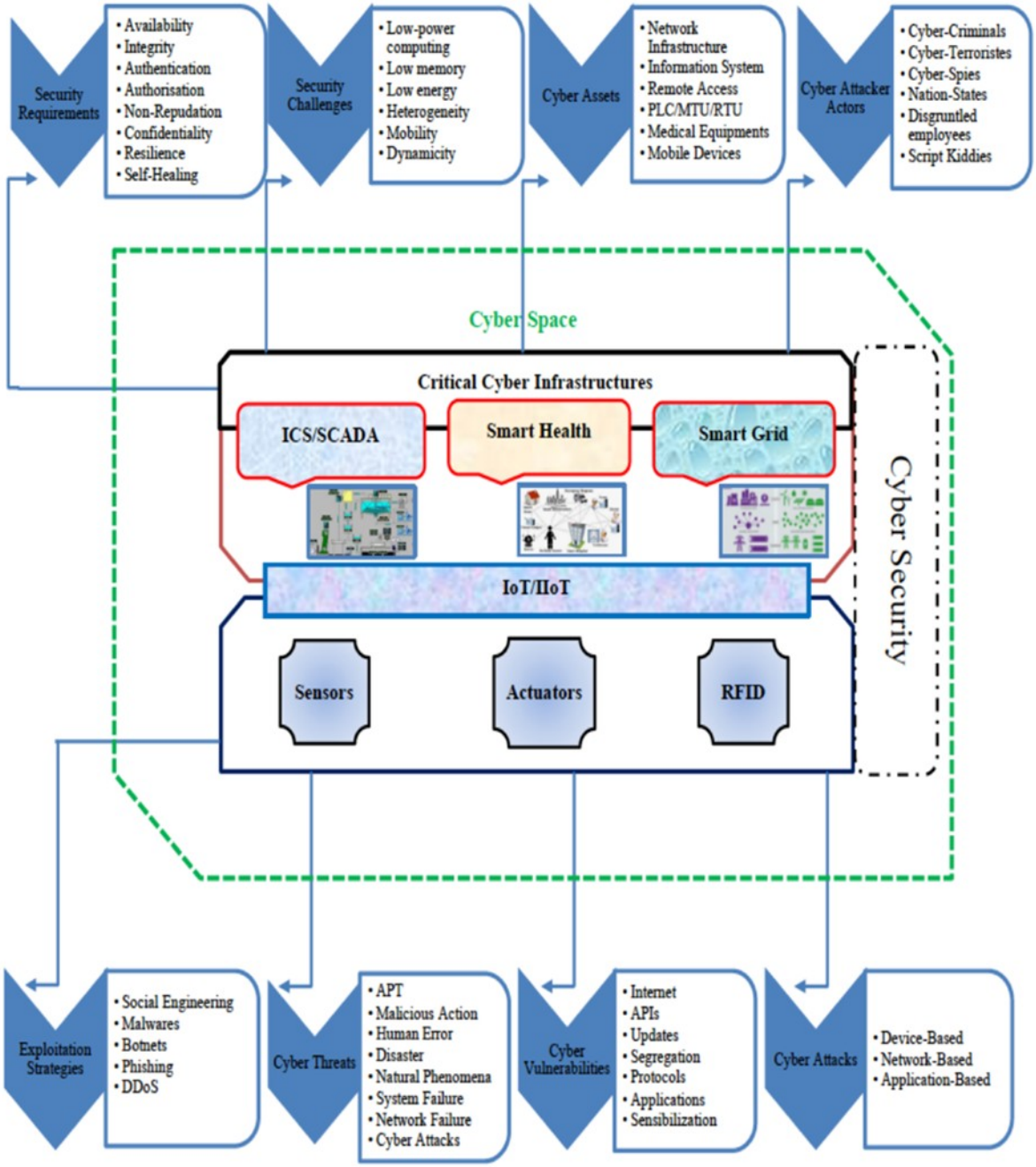

Figure3: Model of the National Cybersecurity Strategy for Critical Infrastructure Objects

The presented model reflects a comprehensive approach to the development of a national cybersecurity strategy for critical infrastructure objects. It demonstrates the interconnection between security requirements, challenges, assets, potential threats, and the roles of key stakeholders. The implementation of such a system ensures the resilience of critical sectors – energy, healthcare, transport, and digital services – through the integration of technical, organizational, and international mechanisms for countering cyber threats.

Thus, the structural model of the National Cybersecurity Center (Fig. 2) serves as the organizational foundation, while the model of the national cybersecurity strategy (Fig. 3) represents the conceptual framework within which this structure operates. The interconnection between them ensures a systemic approach to cyber risk management – from centralized coordination, data collection, and analytics to the implementation of strategic decisions at the sectoral level and among critical infrastructure operators. This approach enables the transition

from a reactive to a proactive cybersecurity model, which is a key prerequisite for building a resilient national security system in the digital environment.

In the context of forming a national cybersecurity strategy, operational readiness and response should be based on a unified incident management procedure that defines clear RACI matrices between operators, sectoral authorities, and the national CERT, as well as standardized reporting formats using TLP, MITRE ATT&CK, and vulnerability taxonomies. Information exchange channels should include tactical (IoC, TTP), operational (response statuses), and strategic (trends) levels [11-12]. It is advisable to implement "SOC as a Service" for small and medium-sized operators, integrate OT telemetry with profiling of normal technological parameters, and automate typical cases – such as phishing, lateral movement, or equipment failure – using SOAR platforms. An important element of enhancing system resilience is regular training and exercises: annual cross-sector tabletop scenarios, technical drills, OT labs for scenario practice, and mandatory recovery simulations with measurable RTO/RPO metrics [15-16].

Public-private partnerships should be implemented through intelligence information sharing platforms (ISAC/ISAO models), operational bulletins with TLP marking, and automation using STIX/TAXII protocols. To encourage voluntary data sharing, it is necessary to introduce "safe harbor" mechanisms and incentives such as tax reliefs, modernization grants for OT, and vouchers for audits and penetration testing. The legal framework of the strategy should define the status of critical infrastructure objects, establish baseline and sectoral cybersecurity control profiles, set clear incident reporting procedures with materiality thresholds, timelines, and sanctions, as well as certification processes aligned with international standards, and mandatory SBOM (Software Bill of Materials) requirements for supply chain security. Protection of personal and critical data is achieved through classification, harmonization of access control regimes, and specific storage requirements [4-6].

It should be noted that an effective national CIF cyber protection strategy is not just a "list of technical measures," but a holistic system of policies, institutions, processes, and competencies. The key consists in the combination of risk-oriented regulation with operational readiness supported by sustainable funding, measurable key performance indicators (KPIs), public-private partnerships, and international cooperation. The proposed model creates a roadmap for increasing the cyber resilience of critical sectors and protecting socially important services in the long term.

3. Conclusion

Thus, the formation of a national strategy for cyber protection of critical infrastructure facilities is a key factor in providing national security, as it allows for systematic risk management, increased resilience of vital services, and reduced consequences of cyberattacks.

The strategy should be based on risk-oriented management, which enables optimal resource allocation and reduced incident response time. The priorities include updating legislation and creating CIF registers; financing cyber protection (NATO countries' spending on cybersecurity increased by an average of 20–25% in 2022–2023); personnel training (Ukraine has a deficit of up to 100 thousand cybersecurity specialists); public-private partnership, since about 80% of CIF belong to the private sector [14].

The expected results are increased cyber resilience of critical sectors, reduced economic losses (which, according to EU estimates, could reach 1.5% of global GDP by 2030 without adequate protection), and strengthened public trust in public institutions [1-2].

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT to: translate certain text fragments into English, perform grammar and spelling checks, and paraphrase or reword content. After using these tools, the authors carefully reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] Polikovska Yu. The number of cyber incidents registered in Ukraine in 2023 increased by 62.5%, - State Special Communications Service, 2024. URL: https://ms.detector.media/internet/post/33956/2024-01-12-kilkist-zareiestrovanykh-v-ukraini-kiberintsydentiv-u-2023-rotsi-zrosla-na-625-derzhspetszvyazku/?utm_source

[2] Holoborodko Ya. The number of cyberattacks in Ukraine increased by 62% in 2023. 2024. URL: https://minfin.com.ua/ua/2024/01/13/119569727/?utm_source

[3] Advancing cybersecurity and resilience of the Union's critical infrastructure. EU Agencies Network. 2025. URL: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors?utm_source

[4] The President of Ukraine approved a new Cybersecurity Strategy of Ukraine. Organization of the National Security and Defense Council of Ukraine, 2021. URL: https://www.rnbo.gov.ua/en/Diialnist/4976.html?utm_source

[5] NIS2 Directive Transposition Tracker URL: https://ecs-org.eu/activities/nis2-directive-transposition-tracker/?utm_source

[6] NIS2 Technical Implementation Guidance. European Union Agency for Cybersecurity (ENISA), 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

[7] Number of cyberattacks on Ukraine increased by 16% in 2023. Economichna Pravda. 2024. URL: https://www.pravda.com.ua/eng/news/2024/01/31/7439720/?utm_source

[8] Number of cyberattacks on Ukraine increased by 70% in past year. Economichna Pravda, 2025. URL: https://www.pravda.com.ua/eng/news/2025/01/9/7492671/?utm_source

[9] Ukraine's energy system under attack. Ukraine's Energy Security and the Coming Winter. URL: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack?utm_source

[10] Ukrainian Cybersecurity Market Quadruples in Eight Years, 2025. URL: https://itukraine.org.ua/en/ukrainian-cybersecurity-market-quadruples-in-eight-years/?utm_source

[11] The Vulnerability Detection and Cyber Incidents / Cyber Attacks Response System helped to detect and process 1,042 cyber incidents in 2024. State Cyber Protection Centre, 2025. URL: https://scpc.gov.ua/en/articles/383?utm_source

[12] Statistical Report on the Results of the Vulnerability Detection and Cyber Incident and Cyberattack Response System Operation for 2023. State Cyber Protection Centre, 2024. URL: https://scpc.gov.ua/en/articles/334?utm_source

[13] Ukraine Leading in Cybersecurity Resilience. IT Association of Ukraine, 2025. URL: https://digitalstate.gov.ua/news/tech/ukraine-leading-in-cybersecurity-resilience?utm_source

[14] Ukraine lacks nearly 100K cybersecurity specialists – special comms agency. Ukrinform, 2025. URL: https://www.ukrinform.net/rubric-society/3976130-ukraine-lacks-nearly-100k-cybersecurity-specialists-special-comms-agency.html?utm_source

[15] Hutsaliuk O., Havrylova N., Alibekova B., Rakayeva A., Bondar Iu., Kovalenko Yu. Management of Renewable Resources in the Energy Sector: Environmental, Economic and Financial Aspects. Green Energy and Technology. Circular Economy for Renewable Energy. Cham: Springer, 2023. 69-89. URL: https://doi.org/10.1007/978-3-031-30800-0

[16] Hutsaliuk O., Bondar Iu., Tomareva-Patlahova V., Kalinin O., Navolokina A., Kozlovska S. Integration of Operational and Economic Security of the Enterprise: Reorganization, Technologies, Risks and Outsourcing. Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies. Cham: Springer, 2025. 240. 35-61. URL: https://doi.org/10.1007/978-3-031-81557-7_3

[17] Hutsaliuk O., Bondar Iu., Kalinin O., Sokolovskiy V., Navolokina A. Integration Development of Logistics Activities of Corporate Enterprises Based on Intellectualization and Management Technologies. Intelligent Transport Systems: Ecology, Safety, Quality, Comfort. ITSESQC 2024. Lecture Notes in Networks and Systems. Cham: Springer, 2025. 1335. 270-289. URL: https://doi.org/10.1007/978-3-031-87376-8_24