POLITYKA ENERGETYCZNA – ENERGY POLICY JOURNAL

2026 ✦ Volume 29 ✦ Issue 2 ✦ 87–112

DOI: 10.33223/epj/213912

Viacheslav Politanskyi[1], Hanna Zaikina[2], Yuliia Mekh[3], Volodymyr Martynovskyi[4], Liliia Pyliuha[5]

Cybersecurity of the energy sector of Ukraine: administrative and legal mechanisms for protecting the state's critical infrastructure

Abstract: This research focuses on the analysis of administrative and legal systems providing cybersecurity within Ukraine's energy sector amidst growing hybrid threats. Utilizing formal legal analysis, comparative methods, systems approaches, and examination of official reports, the study assesses the effectiveness of existing legislation and the roles of critical institutions such as the State Service for Special Communications and Information Protection (SSSCIP), the National Coordination Centre for Cybersecurity (NCSCC), and international cooperation frameworks. The findings indicate that, while Ukraine has made significant strides in developing a foundational legal and

✉ Corresponding Author: Viacheslav Politanskyi; e-mail: viacheslavpolitanskyi@gmail.com

[1] National Academy of Legal Sciences of Ukraine, Ukraine; ORCID iD: 0000-0002-4664-8537; e-mail: viacheslavpolitanskyi@gmail.com

[2] Ukrainian State University of Railway Transport, Ukraine; ORCID iD: 0009-0007-7141-1391; e-mail: h.zaikina@outlook.com

[3] Yaroslav Mudryi National Law University, Ukraine; ORCID iD: 0000-0002-0191-1020; e-mail: ymekh@hotmail.com

[4] Yaroslav Mudryi National Law University, Ukraine; ORCID iD: 0000-0001-5266-8043; e-mail: v-martynovskyi@outlook.com

[5] Yaroslav Mudryi National Law University, Ukraine; ORCID iD: 0000-0002-4267-2062; e-mail: l_pyliuha@hotmail.com

institutional framework aligned with European Union standards, several challenges hinder effective implementation. Key issues include insufficient sector-specific regulations, budgetary limitations, and a critical shortage of professionals with specialized training. The research highlights particular cybersecurity vulnerabilities, such as the protection of automated process control systems and the inconsistent levels of cyber preparedness across energy enterprises. Furthermore, the report underscores the need to enhance governmental oversight, establish clear technical standards that align with IEC 62443 and NIS 2, and expand training and support initiatives for operators of critical infrastructure. The recommendations aim to strengthen Ukraine's energy sector's cyber resilience, ensuring the stability and reliability of national infrastructure amidst rising cyber threats.

Keywords: jurisprudence, global digitalization, operational technologies, international standards, industrial control systems, incident response, international cooperation

Introduction

The energy sector is a critically important component of national security, economic stability, and the societal well-being of any modern state. Its stable and uninterrupted functioning was the foundation for all other spheres of life. In the context of global digitalization, Ukraine's energy infrastructure, as in other countries, demonstrated increasing dependence on information and communication technologies and automated process control systems (APCS). This trend, on the one hand, increased the efficiency and flexibility of energy system management, but on the other hand, created new large-scale risks related to cyber threats (Danchuk and Danchuk 2024; Yasenenko 2025).

The relevance of the study of administrative and legal mechanisms for protecting the cybersecurity of Ukraine's energy sector acquired particular urgency in the context of ongoing full-scale armed aggression, during which critical energy infrastructure objects became priority targets not only for physical attacks but also for targeted cyber operations sponsored by the aggressor state, Russia.

Successful cyberattacks on energy facilities could have led to catastrophic consequences: from mass power outages and disruptions in energy supply to technological accidents, significant economic losses, and the creation of direct threats to citizens' lives and health (Dai et al. 2025; Krechko and Mikhaylov 2025). For this reason, ensuring an appropriate level of cyber resilience in the energy sector was one of the key tasks of the state (Kravchuk et al. 2024). Solving this task was impossible without an effective system of administrative and legal regulation and control.

The problem lay in the fact that the regulatory framework and its application practices often did not adapt to the rapid development of technology and the evolution of cyber threats. Unresolved issues remained regarding the detailing of requirements for the protection of specific systems (e.g., Smart Grids), ensuring effective oversight of the implementation by all operators regardless of ownership form, and effective coordination among the numerous actors

in the national cybersecurity system (Yevdokymov 2025; Biluk et al. 2020). There were gaps in understanding how far the current administrative procedures (licensing, certification, auditing, inspection) and accountability mechanisms could realistically enhance the level of cybersecurity in the sector under conditions of limited resources and constant attacks.

The issue of cybersecurity of critical infrastructure, particularly the energy sector, was actively studied both internationally and nationally. The fundamental aspects of managing the security of critical infrastructure were addressed in the work of Ampratwum et al. (2023), which analyzed public-private partnership models and governance challenges in the context of globalized threats. The specificity of cybersecurity in the energy sector, with a focus on vulnerabilities in automated APCS, was highlighted in technical reports and recommendations by international organizations, such as Industrial Control Systems (ICS), as well as in numerous studies by foreign scholars.

In particular, Alghassab (2022) analyzed the impact of cybersecurity on monitoring and control systems in the energy sector. Khan and Madnick (2021) proposed a systems-theoretic approach called "Cybersafety" for identifying and mitigating cyber vulnerabilities in industrial control systems. Dong et al. (2022) examined the requirements, challenges, and standards of cybersecurity concerning smart local energy systems.

Zografopoulos et al. (2023) provided a review of cybersecurity of Distributed Energy Resources, focusing on the vulnerabilities, potential attacks, consequences, and risk mitigation methods. These issues were also examined in the work of Rajkumar et al. (2023), who modeled cascading effects of cyberattacks on energy systems.

The European approach to regulating the cybersecurity of essential service operators, including energy, through network and information security (NIS) and NIS 2, was analyzed by Singh (2023), who pointed to the challenges of harmonization and ensuring a uniform level of protection across EU member states. European scholars' research more deeply revealed the connection between the single market and EU cybersecurity. For example, Liebetrau (2024) applied the problematization approach, demonstrating how EU single market integration itself functioned as a security practice in the field of cybersecurity.

At the same time, Carrapico and Farrand (2024) examined the latest trends in EU cybersecurity policy through the lens of the regulatory mercantilism concept. The authors argued that the EU, responding to geopolitical instability and digital vulnerabilities, used regulatory measures and cybersecurity standards not only for protection but also for strengthening its digital sovereignty. In Ukrainian academic discourse, the issue of administrative and legal provision for cybersecurity has also received attention.

The work of Zaikina (2024), devoted to administrative and legal support for cybersecurity, analyzed the experience of the United States of America (USA) and the EU in this field. In particular, Zaikina's study emphasized the strategic importance of cybersecurity in the context of hybrid threats. The research by Krykun (2022) revealed that although the Law of Ukraine No. 1882-IX "On critical infrastructure" (2021) was important and timely, some of its provisions contained significant corruption risks.

Kuniev and Krutas (2021) identified the absence of a legal definition of information administrative offenses and major problems with the consistency of regulatory norms in

Ukraine's information sphere. However, despite certain contributions, a comprehensive analysis of administrative and legal mechanisms for protecting Ukraine's energy sector from cyber threats in the context of full-scale war – considering the specifics of operational technology (OT) systems and international standards – remained underdeveloped.

In particular, there was a lack of studies that systematically assessed the effectiveness of the supervisory functions of the State Service of Special Communications & Information Protection of Ukraine (SSSCIP), the effectiveness of licensing and certification procedures in this specific field, and the real problems of law enforcement at the level of critical infrastructure facilities (CIF) operators in the energy sector.

The aim was to explore the effectiveness of administrative and legal regulation of cybersecurity in Ukraine's energy sector. To achieve this aim, the following objectives were set: to analyze the current regulatory and legal framework; to examine the powers and outcomes of the key public authorities; to identify the main problems in law enforcement and the implementation of cybersecurity requirements by energy sector operators; to compare the Ukrainian approach with international experience (EU, USA); and to identify directions for improving administrative and legal mechanisms. This also required understanding key concepts such as "cybersecurity", "critical infrastructure", and "administrative and legal mechanisms".

1. Materials and methods

This study was theoretical in nature and was based on the application of a set of general scientific and specialized cognitive methods aimed at achieving the stated goal. The chronological scope of the analysis covered the development of the regulatory and legal framework and its application practices from 2017 to March 2025, taking into account the key changes and challenges that arose, particularly after the start of full-scale armed aggression in 2022. The year 2017 was chosen as the initial boundary of the study, as it was the year when the Law of Ukraine No. 2163-VIII "On the basic principles of cybersecurity in Ukraine" (2017) was adopted.

The study's source materials included a wide range of documents, such as the regulatory legal acts of Ukraine: the Law of Ukraine No. 2163-VIII "On the basic principles of cybersecurity in Ukraine" (2017), the Law of Ukraine No. 1882-IX "On critical infrastructure" (2021), the Law of Ukraine No. 80/94-VR "On protection of information in automated systems" (1994), the Law of Ukraine No. 2297-VI "On protection of personal data" (2010), the Code of Ukraine "On administrative offences" (1984), the Criminal Code of Ukraine (2001), the Law of Ukraine No. 1366-IX "On amendments to the Code of Ukraine on Administrative Offences and the Criminal Code of Ukraine on strengthening liability for violation of fire and technological safety requirements" (2021), the Law of Ukraine No. 222-VIII "On licensing of economic activity types" (2015), the Law of Ukraine No. 3855-XII "On state secret" (1994), the Law of Ukraine

No. 2019-VIII "On electricity market" (2017), and the Law of Ukraine No. 2229-XII "On Security Service of Ukraine" (1992).

Subordinate acts were also analyzed, including the Resolution of the Cabinet of Ministers of Ukraine No. 444 "On approval of the procedure for training the population to act in emergency situations" (2013), the Order of the Cabinet of Ministers of Ukraine No. 1351-p "On Approval of the Strategy for Digital Development of Innovation Activities of Ukraine for the Period Up to 2030 and Approval of the Operational Action Plan for Its Implementation in 2025–2027" (2024), SSSCIP orders and regulatory documents (Order of the Administration… 2007; Order of the Administration… 2023; Decree of the President of Ukraine No. 447/2021… 2021; Decree of the President of Ukraine No. 242/2016… 2021; Resolution of the Board… 2022).

Access to the text of the acts was obtained through the official database "Legislation of Ukraine" on the website of the Verkhovna Rada of Ukraine. The study's materials also included international legal documents such as the Directives of the European Union, relevant documents of the North Atlantic Treaty Organization (NATO), and international treaties (Convention on Cybercrime (ETS No. 185) 2001; Cyber Resilience Act 2025; Directive (EU) No. 2022/2555… 2022; European Resource Adequacy Assessment 2022 Edition 2022; Regulation (EU) No. 2019/943… 2019; Ukraine-U.S. cooperation… 2022; Relations with Ukraine 2025).

A crucial part of the source base consisted of official reports and analytical materials from the SSSCIP, the National Cyber Security Coordination Centre (NCSCC) under the National Security and Defence Council of Ukraine (NSDCU), the Security Service of Ukraine, as well as reports of international organizations and agencies concerning the state of cybersecurity (Annual analytical review… 2024; Fornusek 2024; The vulnerability detection… 2025). A set of methods was applied to analyze these materials. Among general scientific methods, analysis, synthesis, systematization, and generalization were used to process information, structure data, and formulate conclusions.

Among special legal methods, the formal legal (dogmatic) method played a key role – it was applied to interpret the content of legal norms, analyze the structure, and identify gaps in legislation. Institutional analysis was used to study the powers and interactions of key state bodies in the field of energy cybersecurity, such as the SSSCIP, the NCSCC, the National Energy and Utilities Regulatory Commission (NEURC), and the Security Service of Ukraine (SSU). The comparative legal method was applied to compare Ukrainian approaches with international experience (EU, USA, Israel) in order to identify implementation possibilities for best practices in Ukraine.

Systems analysis was applied to understand administrative and legal mechanisms as a holistic system and to explore the interconnections among its institutional, regulatory, and procedural components. The selection of the above materials and methods was justified by the theoretical nature of the study and its objective, which required an in-depth analysis of the regulatory and legal framework, a generalization of available information on its application practices, and a comparison with academic doctrine and international experience.

2. Results and discussion

SSSCIP, since 2022, has been maintaining an updated national registry of critical infrastructure in Ukraine's energy sector. This registry plays a pivotal role in enhancing the cybersecurity oversight of the sector, and including this information would ground the article's findings in the broader context of national efforts to combat cyber threats.

As of March 2025, the administrative and legal mechanisms for protecting cybersecurity in Ukraine's energy sector represented a complex system of regulatory governance and institutional support, which remained in a state of active transformation and adaptation to modern challenges – particularly under conditions of ongoing full-scale armed aggression by Russia against Ukraine. There existed a need to improve the administrative and legal framework to preserve the integrity, availability, and confidentiality of data and control systems in the energy sector, to minimize the risks of large-scale disruptions, economic losses, and national security threats caused by cyberattacks (Tsybka 2025; Işık et al. 2025b). Cyber threats to Ukraine's energy sector were characterized by diversity: from attacks aimed at espionage and data theft to destructive attacks on APCS and OT, aimed at physically damaging equipment or disrupting energy supply (The vulnerability detection… 2025).

Particularly dangerous were targeted advanced persistent threats (APT) sponsored by the aggressor state, which exploited software vulnerabilities, social engineering, and supply chain attacks to penetrate the networks of energy companies (Annual analytical review… 2024; Fornusek 2024). In response to these threats, Ukraine formed a multi-level system of administrative and legal protection. The key body in this system was the SSSCIP, which was assigned the functions of forming and implementing state policy in the fields of cyber protection, cryptography, and technical information security.

Throughout 2024–2025, the SSSCIP actively carried out supervisory and oversight activities regarding the state of cybersecurity of CIF in the energy sector, including transmission system operators such as the National Energy Company (NEC) "Ukrenergo", distribution system operators, generating companies, as well as oil and gas enterprises (e.g., the gas transmission system operator) (Order of the Administration… 2023). These activities were conducted on the basis of the Law of Ukraine No. 2163-VIII "On the basic principles of cybersecurity in Ukraine" (2017), which, in particular, defined the powers of the SSSCIP to exercise state control over the state of cyber protection of state information resources and information subject to legal protection, as well as the Computer Emergency Response Team of Ukraine (CERT-UA), and the Law of Ukraine No. 1882-IX "On Critical Infrastructure" (2021).

The latter law detailed the process of identifying and categorizing critical infrastructure objects (the energy sector was classified as vital), and the requirements for the security passports and protection plans, which were required to include cyber protection measures (Articles 9, 10, 22, 24). Based on detected violations, the SSSCIP issued mandatory orders for rectification within a set timeframe and monitored the implementation, which constituted a direct manifestation of administrative and legal enforcement.

Liability for failure to comply with these orders, as well as for violations of legislation on cybersecurity and critical infrastructure protection, was significantly strengthened, particularly through the Law of Ukraine No. 1366-IX "On Amendments to the Code of Ukraine on Administrative Offences and the Criminal Code of Ukraine on Strengthening Liability for Violation of Fire and Technological Safety Requirements" (2021), which amended the Code of Ukraine "On Administrative Offences" (1984).

The increase in fines under Article 188-8 of the Code aimed to raise the level of accountability among CIF operator officials. For instance, failure to comply with lawful demands from SSSCIP officials to rectify violations of critical infrastructure protection legislation could result in a fine of one hundred to two hundred non-taxable minimum incomes of citizens, and in the case of repeat offenses within a year, from two hundred to three hundred. This underscored the administrative and legal dimension of ensuring compliance with cybersecurity regulations.

In addition to administrative liability, criminal liability was also provided for under Section XVI of the Criminal Code of Ukraine (2001) for unauthorized interference with the operation of information, electronic communication, or information and communication systems, or electronic communication networks (Article 361); creation of malicious software or technical means (Article 361-1); the distribution (Article 361-2); and other cybercrimes that could have been directed against energy infrastructure.

The coordinating role in the national cybersecurity system was played by the NCSCC, the operational body of the NSDCU. As of March 2025, the NCSCC continued to ensure coordination and oversight of the activities of security and defense sector entities and other state authorities in the field of cybersecurity, analysis of the cybersecurity situation, and forecasting and detection of potential and actual cyber threats to national security.

The NCSCC's activities were based on the Decree of the President of Ukraine No. 242/2016 "On the National Coordination Centre for Cybersecurity" (2021), approved by the Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 "On the Cybersecurity Strategy of Ukraine"" (2021), which replaced the previous strategy from 2016.

In 2024, the NCSCC, together with other cybersecurity actors, worked on the implementation of the action plan of the Strategy, paying particular attention to the protection of critical information infrastructure (CII), which included information systems in the energy sector. A key element of the NCSCC's activities was the organization of cyber incident information sharing between public authorities, critical infrastructure operators, and international partners through the MISP-UA Cyber Incident Information Sharing Platform, the functioning of which was regulated by relevant normative acts (On sharing information on cyber threats 2022).

This multi-actor model of cybersecurity governance, in which the NCSCC played the coordinating role and the SSSCIP held the main regulatory and supervisory functions, aligned with global practices of establishing specialized state agencies and coordination centers. The study by Agyemang et al. (2025) on cybersecurity governance models in EU countries also emphasized the importance of a clear division of powers between various state bodies and the need for effective interagency coordination – an issue relevant to Ukraine as well.

The role of the SSSCIP as the central authority in the field of technical information protection and cybersecurity correlated with the functions of analogous agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) in the USA or the British Standards Institution in Germany, as analyzed in the comparative study by Odebade and Benkhelifa (2023). The SSSCIP issued licenses for economic activities involving cryptographic information protection services (except for digital signature services) and technical information protection (TIP), pursuant to the Law of Ukraine No. 222-VIII "On Licensing of Economic Activity Types" (2015) and the Licensing Conditions for providing services in the field of technical information protection (as defined by the Cabinet of Ministers of Ukraine), approved by Resolution No. 444 "On Approval of the Procedure for Training the Population to Act in Emergency Situations" (2013). This enabled the state to monitor the quality of services provided to energy sector entities in the field of cyber protection and to establish qualification requirements for service providers.

Moreover, the SSSCIP conducted state expertise and issued conformity certificates for integrated information protection systems (IIPS) in information and communication systems that processed legally protected information. For critical infrastructure objects, the presence of a certified IIPS was a mandatory requirement (Law of Ukraine No. 2163-VIII… 2017).

The procedure for conducting state expertise was defined by the Regulation on State Expertise in the Field of Technical Information Protection, approved by Order No. 93 of the SSSCIP "On Approval of the Regulation on State Expertise in the Field of Technical Information Protection" (2007). The SSSCIP also certified cryptographic and technical information protection tools for compliance with the requirements of the technical information protection system's normative document. The use of uncertified tools for protecting state information resources or restricted-access information was prohibited.

The importance of the Law of Ukraine No. 2297-VI "On Protection of Personal Data" (2010) should also be noted, as energy companies (suppliers, network operators) processed large volumes of consumer personal data. Ensuring the confidentiality and protection of this data from unauthorized access or leakage was an integral part of the overall cybersecurity system, and violations of the requirements of this law also carried administrative liability. Additionally, the Law of Ukraine No. 3855-XII "On State Secret" (1994) established requirements for the protection of information classified as state secrets, which could include the operational schemes of critical energy objects, the protection systems, etc.

A key aspect of administrative and legal support was the professional development of specialists. In 2024–2025, the SSSCIP continued to implement training and upskilling programs for cybersecurity professionals working in the energy sector. These included large-scale simulation exercises replicating cyber incidents at power plants and transmission centers, as well as real-world scenario-based drills for incident response and SCADA protection. The programs were implemented in cooperation with international partners, including the U.S. Embassy in Ukraine, the Estonian e-Governance Academy, and ENISA experts. These programs included training sessions, seminars, and courses, including those focused on APCS protection, incident response, and security audits. For example, specialized courses were conducted at SSSCIP training centers with the involvement of international partners.

Other state bodies also played a role. The Ministry of Energy of Ukraine was responsible for shaping sectoral policy, including cybersecurity aspects in the energy field, and promoted the implementation of appropriate standards and practices at sector enterprises, interacting with the SSSCIP on the development of sectoral requirements. The Law of Ukraine No. 2019-VIII "On Electricity Market" (2017) established general requirements for the reliability and safety of market operation, which indirectly included the cybersecurity of operational activities of its participants.

Within its powers, the NEURC could establish reliability and safety requirements for energy system licensees, which indirectly concern cybersecurity – for example, through licensing conditions. The SSU carried out counterintelligence activities in the cybersecurity field, investigated cybercrimes targeting critical infrastructure, and countered cyberterrorism and cyber espionage, including from the intelligence services of the aggressor state, Russia (Law of Ukraine No. 2229-XII… 1992).

Although the Ministry of Digital Transformation of Ukraine did not have direct regulatory influence over the energy sector, it contributed to the overall increase in cyber literacy and the implementation of secure digital technologies in the economy through national programs such as the Digital Transformation Programme to 2027, approved by Order No. 1351-p of the Cabinet of Ministers of Ukraine "On Approval of the Strategy for Digital Development of Innovation Activities of Ukraine for the Period Up to 2030 and Approval of the Operational Action Plan for Its Implementation in 2025–2027" (2024).

The National Bank of Ukraine (NBU) established strict cybersecurity requirements for the banking system, which indirectly had a positive impact on the financial stability of energy companies and the protection of the financial operations (Resolution of the Board… 2022). These requirements included mandatory implementation of Information Security Management Systems (ISMS) based on international standards, regular penetration testing and audits, as well as clear procedures for incident reporting. For better visual comparison of the key regulatory acts of Ukraine in the field of cybersecurity for the energy sector, Table 1 was created.

Particular attention within the framework of administrative and legal regulation was paid to the protection of APCS, also known as OT or ICS. Cyberattacks on APCS of energy facilities (power plants, substations, dispatch centers) could have had catastrophic consequences, including large-scale blackouts (as observed in Ukraine in 2015-2016), damage to expensive equipment, and threats to human life and health (Assante 2016; Semenenko et al. 2024). As of March 2025, the regulatory and legal framework regarding APCS protection was still in an active stage of development.

General requirements were contained in the Law of Ukraine No. 2163-VIII "On the basic principles of cybersecurity in Ukraine" (2017) and the Law of Ukraine No. 1882-IX "On critical infrastructure" (2021), but there was a lack of detailed sectoral standards that would take into account the specifics of APCS in the energy sector, including the absence of official guidelines for OT network segmentation, PLC security configuration and patching, and incident communication and escalation protocols. The lack of these detailed frameworks limited the uniform implementation of cybersecurity measures across enterprises and complicated

Table 1. Key regulatory and legal acts of Ukraine in the field of cybersecurity of the energy sector

Tabela 1. Najważniejsze akty prawne Ukrainy w dziedzinie cyberbezpieczeństwa sektora energetycznego

Name of the act	Number/date	Key provisions for the energy sector and administrative and legal regulation
Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine"	No. 2163-VIII/05.10.2017	Defines the legal and organizational framework for ensuring the protection of the vital interests of a person and a citizen, society and the state, and the national interests of Ukraine in cyberspace, the powers, and duties of state bodies, enterprises, institutions, organizations, including CII operators. Establishes the principles of coordination.
Law of Ukraine "On Critical Infrastructure"	No. 1882-IX/16.11.2021	Defines the legal and organizational framework for the creation and functioning of the national critical infrastructure protection system, classifies energy facilities as CII, establishes requirements for the protection, including cyber defense, responsibilities of CII operators, and powers of authorized bodies (including the SSSCIP).
Law of Ukraine "On Technical Protection of Information"	No. 2297-VI/01.06.2010	Regulates relations in the field of technical information protection (TIP), establishes requirements for TIP means and complexes, the procedure for the examination and certification. It applies to information whose protection is required by law.
Law of Ukraine "On Protection of Information in Automated Systems"	No. 80/94-VR/05.07.1994	Establishes general principles of information protection in ICS, rights and obligations of owners of systems and information, and liability for violations.
Criminal Code of Ukraine	No. 2341-III/05.04.2001	Establishes criminal liability for crimes in the field of use of electronic computers, systems, and computer networks and telecommunication networks (Section XVI)4, in particular for unauthorized interference with the operation of ICS that caused significant damage or led to serious consequences.
Code of Ukraine "On Administrative Offences"	No. 8073-X/07.12.1984	Establishes administrative liability for violations in the field of information protection, in particular, Article 188-8 for violation of CII protection legislation and failure to comply with SSSCIP requirements.
CMU Resolution	No. 564/ 10.07.2020	Approves the procedure for the functioning of the national cybersecurity system, defines the interaction of the main cybersecurity actors (NCSCC, SSSCIP, SSU, NPU, Ministry of Defence, intelligence agencies, NBU), and procedures for exchanging information on cyber incidents.
Presidential Decree	No. 447/2021/ 26.08.2021	Approves the cybersecurity strategy of Ukraine, defines priorities, goals, and objectives of the state policy in this area, particularly the protection of CII.
SSSCIP Order	No. 321/ 15.06.2024	Approves requirements for information protection in information systems of critical infrastructure facilities, detailing technical and organizational measures to be implemented by CIF operators in the energy sector.
SSSCIP Order	No. 678/20. 12.2024	Approves additional requirements for cybersecurity of critical information infrastructure facilities in the energy sector aimed at countering state cyberattacks, taking into account the specifics of threats.

Source: compiled by the authors.

compliance verification. In 2024, the SSSCIP initiated the development of such sectoral standards in cooperation with the Ministry of Energy, representatives of energy companies, and cybersecurity experts.

The work by Markopoulou et al. (2019) showed that the general requirements of the directive required specification at the national and sectoral level for effective application by operators of essential services, particularly in energy. The need to develop such detailed sectoral standards was confirmed by international practice and research. The use of international standards such as IEC 62443 and the NIST Cybersecurity Framework as a basis for developing Ukrainian sectoral norms aligned with the best global practices, as demonstrated by the research of Malatji et al. (2022) on standardization in the field of CII cybersecurity.

An important administrative mechanism for monitoring APCS protection status was the SSSCIP inspections, during which the architecture of OT networks, security settings of controllers (PLC), human-machine interfaces, Supervisory Control and Data Acquisition (SCADA) systems, availability of security monitoring tools, and incident response procedures in the technological segment were analyzed. However, the effectiveness of such control was limited by a shortage of SSSCIP specialists with deep knowledge in the security of industrial control systems.

There was also the issue of insufficient funding for APCS protection measures at many enterprises, particularly those using outdated equipment whose modernization required substantial investment. These challenges related to the regulation of OT and ICS security were a global problem. The works of Striolo and Huang (2022), devoted to APCS security in energy, pointed to similar issues: outdated equipment use, difficulties in applying standard IT security solutions in OT environments, and a lack of qualified personnel combining knowledge of IT, OT, and industry-specific context.

The problem identified in Ukraine of insufficient segmentation between IT and OT networks was also recognized as one of the key vulnerabilities in the report by Lella et al. (2023) and in studies by international experts such as Firoozjaei et al. (2022), who analyzed incidents in industrial systems.

The development of new technologies in energy, such as Smart Grids, widespread implementation of renewable energy sources (RES) with the management systems, development of Energy Storage Systems, use of the Internet of Things (IoT) for monitoring and control, as well as migration to cloud platforms, created new cybersecurity challenges and required adaptation of administrative and legal mechanisms. Smart Grids, combining traditional energy infrastructure with information and communication technologies, significantly expanded the attack surface. The large number of connected devices (smart meters, sensors, controllers) created new entry points for attackers. As of 2025, the cybersecurity regulation of Smart Grids in Ukraine remained at an early stage.

Concepts and strategies for the development of Smart Grids were being developed, which envisaged cybersecurity requirements, but specific technical regulations and standards still required approval. The SSSCIP and the Ministry of Energy studied international experience, including EU directives and standards, for example, Regulation (EU) No. 2019/943 of the European Parliament and of the Council “On the Internal Market for Electricity” (2019),

which included references to cybersecurity; Directive (EU) No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union" (2022), which strengthened risk management and incident reporting requirements for the energy sector; and NIST standards (e.g., NIST Framework for Improving Critical Infrastructure Cybersecurity, NISTIR 7628 Guidelines for Smart Grid Cybersecurity). Harmonization with NIS 2 required Ukraine to implement a risk-based approach, introduce supply chain security measures, strengthen incident reporting obligations (within 24 hours – early warning; within 72 hours – incident report), and establish stricter sanctions for non-compliance.

Cybersecurity of RES facilities and energy storage systems also required separate attention, as these systems were often remotely controlled and integrated into the general energy system. The vulnerability could lead to the destabilization of the energy system. Similarly, the use of IoT devices and cloud services in energy requires the establishment of clear security requirements, including secure development, testing, configuration, update management, and data protection, potentially falling under the scope of future requirements similar to the European Cyber Resilience Act (2025).

Administrative and legal mechanisms had to ensure that energy sector operators, when implementing new technologies, adequately assessed cybersecurity risks and took appropriate protective measures, which should have been reflected in the critical infrastructure protection plans and subject to verification by the SSSCIP. A unique aspect of the Ukrainian situation that significantly affected administrative and legal mechanisms – and had no full analog in peacetime studies – was the ongoing full-scale military aggression and the use of cyberattacks as a tool of hybrid warfare on an unprecedented scale. In response, administrative practice increasingly prioritized operational continuity over procedural compliance, emphasizing rapid incident response, redundant system operation, and coordination with intelligence and military cyber units. These wartime adaptations reshaped risk assessment and resource allocation, integrating defense imperatives into civilian cybersecurity governance.

As noted by Ukrainian researchers, such as Hrynchyshyna (2024), the energy infrastructure was one of the priority targets for state-sponsored attacks. This required the Ukrainian cyber defense system not only to meet general standards but also to be capable of withstanding complex, targeted APT-level attacks, which demanded significantly higher resilience standards, faster response, and closer integration with the intelligence community and international partners. This military dimension could explain certain differences in priorities and speed of implementation of measures compared to countries developing the cybersecurity systems under more stable conditions, as analyzed by, for example, Sulich et al. (2021).

Cybersecurity audit procedures required by legislation were to be conducted regularly (usually at least once every two years for CIF) with the involvement of licensed auditors or by internal staff, provided such staff had qualified personnel and an approved methodology. The audit methodology had to be based on national standards, such as Ukrainian State Standards (DSTU), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, DSTU ISO/IEC 27002, and the requirements of regulatory documents of the technical information protection system.

In practice, such audits could include OT network architecture verification, PLC and SCADA systems analysis, penetration testing, and assessment of comprehensive information protection systems, proper network segmentation, legacy equipment vulnerability management, and incident response planning. Audit reports were to be submitted to the SSSCIP. International cooperation played an extremely important role in strengthening cybersecurity in Ukraine's energy sector (Tanasiichuk et al. 2024; Işık et al. 2025a).

During 2024-2025, Ukraine actively developed partnerships in this area with key international players and organizations. Cooperation with the United States of America remained strategic. Within bilateral agreements, such as the Memorandum of Cooperation on Cybersecurity with CISA, and through assistance programs from USAID and the U.S. Department of State, Ukraine received technical support, expert assistance, and equipment for critical infrastructure protection (Ukraine-U.S. cooperation… 2022).

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) provided threat intelligence, vulnerability data, and best practices for ICS/SCADA system protection (CISA Advisories, updated regularly). Cooperation with the European Union has also developed actively. Ukraine, as an EU candidate country, harmonized its legislation with European norms, particularly with Directive (EU) No. 2022/2555 (2022).

Significant support in digital transformation and resilience strengthening over the previous four years was provided by the EU-funded EU4DigitalUA project (2025), implemented by institutions including the Estonian e-Governance Academy, completing its main phase by March 2024 (The European Union supports… 2024). The project contributed to the development of digital infrastructure, including the modernization of ten national registers and the support and scaling of the Trembita electronic data exchange system, which enabled billions of secure exchanges.

The project also supported harmonization of Ukrainian trust services with EU standards – vital for secure cross-border digital interaction. The Electronic IDentification, Authentication and Trust Services (eIDAS) Regulation (2025) established a unified legal framework for key services such as electronic identification, e-signatures, e-seals, time stamps, e-delivery, and website authentication certificates.

In the field of cybersecurity, the project held several rounds of practical cyber exercises and developed recommendations for cyber threat information sharing, which contributed to legislative harmonization with EU norms and enhanced response capabilities to large-scale cyberattacks during martial law. It also developed a subsystem for monitoring access to personal data to enhance citizen control over their own information (The European Union supports… 2024).

In particular, the EU allocated EUR 10 million to support the needs of Ukrainian state bodies in cybersecurity (EU supports cybersecurity… 2022). Ukraine signed a cooperation agreement with the European Union Agency for Cybersecurity (ENISA), which provided for information exchange on incidents, joint exercises, and access to ENISA methodologies (Safeguarding cyberspace together… 2023). Ukraine's integration into the European Network of Transmission System Operators for Electricity (ENTSO-E) in March 2022 set new cybersecurity requirements (European Resource Adequacy Assessment 2022 Edition 2022).

NEC "Ukrenergo" and other operators had to comply with ENTSO-E standards and operational security rules and data exchange (e.g., ENTSO-E Operational Security Network Code), which required constant improvement of protection systems and participation in ENTSO-E joint cybersecurity activities. Cooperation with NATO also remained important. Ukraine, as a NATO Enhanced Opportunities Partner, participated in Alliance programs and cybersecurity exercises, such as the annual Locked Shields drills organized by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.

NATO provided Ukraine with advisory and practical assistance in strengthening cyber defense, particularly through the NATO Cyber Defence Trust Fund (Relations with Ukraine 2025). In addition, Ukraine cooperated with the Organisation for Security and Co-operation in Europe (OSCE) under confidence-building measures in cyberspace and with the Council of Europe in the implementation of the Convention on Cybercrime (ETS No. 185) (2001).

Bilateral experience exchange with countries having advanced energy infrastructure protection practices, such as Israel (with its integrated CII protection system under the National Cyber Directorate) and the United Kingdom (NCSC), was also important. Administrative and legal mechanisms envisaged formalizing such cooperation through international treaties, memoranda of understanding, participation in international information-sharing platforms (e.g., via CERT-UA), and joint working groups (On sharing information on cyber threats 2022).

The importance of international cooperation and harmonization with EU law (in particular, NIS 2 implementation) identified in the study fully corresponded with the conclusions of European and Ukrainian experts, such as Brunet-Jailly (2022), Krimmer et al. (2021), Casino et al. (2022), Savchuk (2024), that the cross-border nature of cyber threats required joint efforts and common standards.

Successful integration into ENTSO-E and adaptation to its cybersecurity requirements was an important step, although it created additional challenges for Ukrainian operators, as shown by studies of the European energy market, such as Korosteleva (2022), Weber (2023), Osička and Černoch (2022). Figure 1 schematically depicts the main actors of administrative and legal support for cybersecurity in Ukraine's energy sector as of March 2025.

Despite significant efforts and progress in building the cybersecurity system of the energy sector, a number of key issues and challenges requiring resolution were identified as of March 2025. There existed a problem of insufficient harmonization and detailing of the regulatory and legal framework. Although the main laws had been adopted, there was a lack of subordinate acts and sectoral standards that would clearly define specific technical and organizational requirements for the cyber protection of different types of energy facilities, especially concerning APCS and emerging technologies (Smart Grids, IoT). This created legal uncertainty for operators and complicated control by the SSSCIP. There was an uneven level of cybersecurity across different enterprises in the sector.

Large state-owned companies, such as the transmission system operator NEC "Ukrenergo", and some private operators had better resources and implemented more modern protection systems, whereas many smaller enterprises, particularly in the electricity distribution sector and among generating companies (especially those working with renewable energy sources – RES),

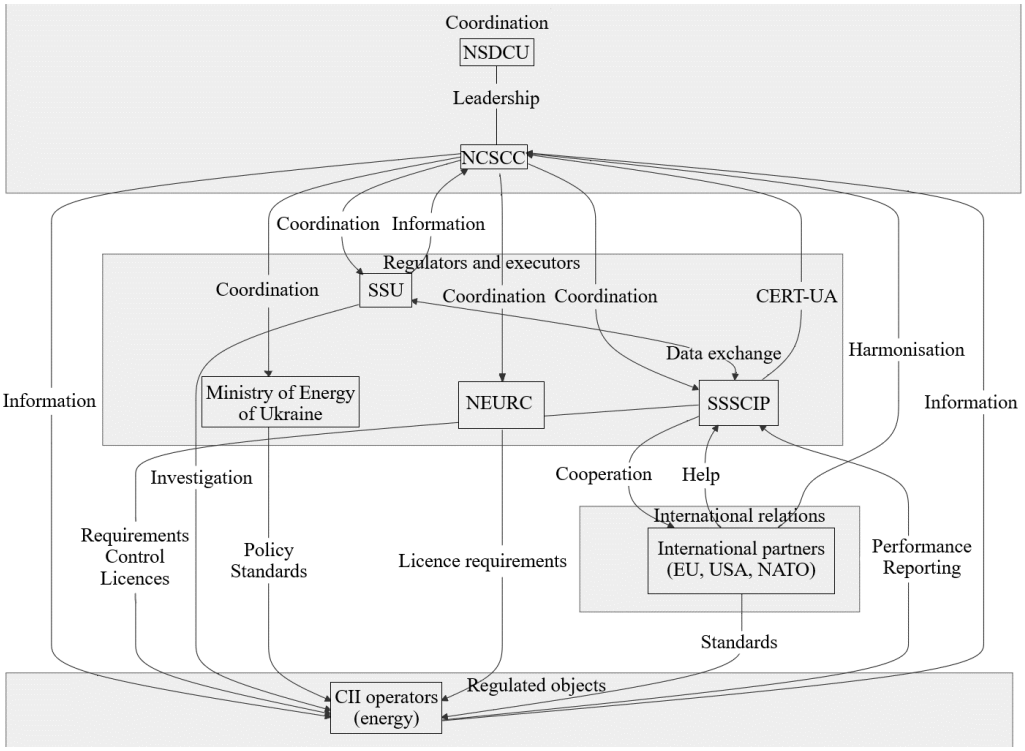

Fig. 1. Schematic representation of the main subjects of administrative and legal support of cybersecurity in the energy sector of Ukraine
Source: compiled by the authors

Rys. 1. Schemat przedstawiający główne obszary wsparcia administracyjnego i prawnego w zakresie cyberbezpieczeństwa w sektorze energetycznym Ukrainy

had limited financial and human capacity to ensure an adequate level of cybersecurity. This created weak points in the energy system that could be exploited by attackers for cascading attacks. There was a shortage of qualified personnel in the field of cybersecurity, both in energy sector enterprises and in state authorities responsible for regulation and control.

There was a particular lack of specialists who combined knowledge in IT security, APCS security, and the specifics of energy processes. The insufficient level of staff training at all levels remained one of the main vulnerabilities. This problem was also a global trend, as evidenced by annual reports from organizations such as (Parkes et al. 2024). The need to strengthen training and retention programs for personnel, highlighted as a conclusion of the study, coincided with the recommendations of researchers such as Pollini et al. (2022) regarding strategies for developing human potential in cybersecurity.

Insufficient funding for cybersecurity measures remained a serious obstacle. In the context of economic difficulties caused by the war and the need to restore physically damaged

infrastructure, cybersecurity expenditures were often not prioritized, especially at enterprises with limited resources (Li and Tian 2024; Anguelov and Kavaldzhieva 2021). The effectiveness of state control and supervision needs to be strengthened.

Despite the increase in the number of SSSCIP inspections, the depth and coverage, particularly regarding APCS, could have been insufficient due to a lack of resources and specialized knowledge among inspectors. Specifically, many inspectors lacked advanced technical expertise in ICS security, sufficient legal authority for on-site technical verification, and an adequate workforce to conduct comprehensive audits across all critical infrastructure facilities. These deficits constrained the state's ability to detect vulnerabilities in OT environments and to enforce timely corrective measures. The system of accountability for cybersecurity violations also required improvement to ensure that it was unavoidable and acted as a deterrent; in addition, judicial practice concerning liability for cybercrimes against CII was limited due to the complexity of attributing attacks and collecting evidence. Improvements were particularly needed in oversight mechanisms, such as independent review boards and inter-agency audit procedures, as well as in legal enforcement tools enabling swifter prosecution of non-compliant operators. Judicial practices were constrained by limited cyber-forensic capacity, outdated procedural norms, and the absence of specialized judicial training in cybersecurity-related cases.

Coordination between different actors in the national cybersecurity system, although improved with the strengthened role of the NCSCC, still requires refinement, especially in terms of the speed of tactical threat information exchange and real-time incident response. The high intensity and complexity of cyberattacks, particularly those sponsored by the aggressor state Russia, demanded constant updates of protection tools, response tactics, and deepened international cooperation to access up-to-date threat intelligence and advanced protection technologies (Onykiienko and Mazin 2025).

To overcome the identified problems, it was necessary to accelerate the development and adoption of subordinate acts and detailed sectoral cybersecurity standards for the energy sector, particularly for APCS and Smart Grids, harmonized with international standards (IEC 62443, NIST) and EU requirements (NIS 2). It would be important to introduce state support mechanisms (financial, technical, methodological) for small and medium energy sector operators to implement mandatory cyber protection measures, possibly through targeted programs or tax incentives.

It would also be necessary to significantly expand training and professional development programs for cybersecurity specialists in the energy sector, particularly by creating specialized training programs at higher education institutions and training centers, possibly in partnership with international organizations and the private sector, as well as introducing staff certification programs.

It would also be necessary to strengthen the institutional capacity of the SSSCIP and other supervisory bodies by increasing the number of qualified inspectors, training, and providing them with the necessary technical tools for conducting in-depth cybersecurity audits, including penetration testing and APCS security analysis. It would be appropriate to improve coordination and information exchange mechanisms among all cybersecurity stakeholders, particularly

through the further development of the MISP-UA platform, ensuring its interoperability with international platforms, and creating a fully-fledged sectoral information sharing and analysis center for cybersecurity threats in the energy sector (Energy ISAC/CERT-UA).

It would also be necessary to continue and deepen international cooperation, particularly in the field of real-time cyber threat intelligence exchange, joint cyberattack investigations, technical assistance, and participation in international exercises and resilience-building programs. The administrative and legal mechanisms for cybersecurity protection in Ukraine's energy sector as of March 2025 represented a dynamic system evolving under the influence of legislative changes, institutional reforms, and growing cyber threats, yet required further systemic improvement at the regulatory, institutional, technical, and human resource levels to ensure an adequate level of resilience of the state's critical infrastructure.

The conducted study of the administrative and legal mechanisms for protecting cybersecurity in Ukraine's energy sector revealed the presence of a comprehensive, albeit still evolving, system of regulatory governance and institutional support. The results of the analysis indicated the existence of a legislative framework that included key laws on cybersecurity and critical infrastructure, the designation of the main responsible entities (in particular, SSSCIP, NCSCC, SSU, CIF operators), as well as the introduction of mechanisms for control, licensing, and certification.

At the same time, significant challenges were identified relating to the practical implementation of requirements, insufficient detailing of sectoral standards, particularly for OT and advanced systems (Smart Grids, IoT), uneven levels of protection among different operators, a shortage of qualified personnel and resources, and the need for constant adaptation to the unprecedentedly high level of cyber threats in the context of full-scale aggression.

International cooperation and the process of harmonization with EU norms played a significant role in strengthening capabilities. The significance of the obtained results lies in highlighting the current state of administrative and legal support for cybersecurity in a strategically important sector of Ukraine's economy and identifying critical gaps requiring urgent resolution. The functioning of the energy sector was a guarantee not only of economic stability but also of national security and societal livelihood, especially in wartime (Boiko et al. 2023; Kuznietsova et al. 2022).

Therefore, the effectiveness of administrative and legal mechanisms for its cybersecurity has acquired exceptional priority. The identified problems, such as insufficient protection of APCS or a formal approach to risk assessment at certain enterprises, indicated potential vulnerabilities that could be exploited for destructive attacks with severe consequences, as had already been demonstrated by incidents in previous years (Assante 2016; Umair and Guliyeva 2025). The successful functioning of the state control system, adequacy of regulatory requirements, and the strict enforcement were critically important for minimizing these risks.

Conclusions

As a result of the conducted study on the administrative and legal mechanisms for protecting cybersecurity in Ukraine's energy sector, it was established that the country had formed the basic legislative and institutional foundations for ensuring the cyber resilience of this critically important industry. A coordination system functioned under the leadership of the NCSCC, and the key regulator and supervisory authority – the SSSCIP – was designated and endowed with the relevant powers.

The regulatory framework, which included laws on cybersecurity and critical infrastructure, laid the foundation for building a national protection system. However, the analysis revealed a significant gap between the formal legal establishment of mechanisms and the effectiveness of the practical implementation. These discrepancies stem from several systemic factors. Bureaucratic inertia, fragmented institutional responsibilities, and limited interoperability between legacy and modern control systems often slow the translation of legal norms into operational practices. In addition, competing financial and operational priorities within energy enterprises tend to relegate cybersecurity to a secondary position, undermining the consistent execution of regulatory requirements.

It was found that the effectiveness of the existing system was limited by a number of systemic problems: insufficient detailing and updating of regulatory requirements, especially regarding specific technologies (APCS, Smart Grids); uneven levels of implementation of cyber protection measures by CIF operators, particularly due to lack of resources and qualifications; inadequate capacity of state control mechanisms to ensure thorough audits and strict compliance by all entities; and a shortage of specialized personnel. To strengthen accountability and ensure measurable progress, it would be advisable to introduce key performance indicators (KPIs) for cybersecurity compliance and resilience across critical infrastructure facilities. Regular independent audits based on these KPIs, with transparent reporting to designated stakeholders, would enable objective assessment of institutional performance and promote a culture of continuous improvement.

Thus, despite the presence of formal prerequisites, the existing administrative and legal mechanisms did not fully correspond to the level and nature of modern cyber threats, especially under conditions of unprecedented external pressure. The obtained results underscored the urgent need to improve the system of administrative and legal support for cybersecurity in the energy sector.

In view of this, it was recommended to accelerate the development and implementation of detailed sectoral standards and technical cybersecurity regulations for the energy sector, harmonized with international norms (such as IEC 62443). It was necessary to strengthen the institutional capacity of the SSSCIP to exercise effective control, in particular by improving the qualifications of inspectors in the field of OT security and introducing a risk-based approach to inspections.

It was deemed appropriate to introduce state support programs for CIF operators (especially small and medium-sized) for the modernization of protection systems. Further development of public-private partnerships and platforms for sharing information about threats and incidents, such as sectoral ISACs, was considered important. Priority attention was needed to address the issue of personnel shortages by reforming the education and professional training system for cybersecurity specialists in the energy sector.

A significant limitation of the conducted study was the incompleteness of the available empirical base. This was due to the confidential nature of data on the actual state of cyber protection, incidents, and security measures at specific critical energy infrastructure facilities. Limited access to such detailed information affected the depth of analysis of the practical aspects of implementing administrative and legal mechanisms and the ability to verify certain conclusions.

Promising areas for further research in this field included: in-depth analysis of the effectiveness of specific administrative procedures (for example, the impact of licensing or the effectiveness of audits); comparative case studies on the implementation of cybersecurity at different types of energy enterprises; and the development of administrative and legal approaches to regulating cybersecurity of emerging technologies (AI, quantum computing) in the energy sector.

The Authors have no conflicts of interest to declare.

References

Agyemang et al. 2025 – Agyemang, R., Furnell, S. and Muller, T. 2025. A profile-based cyber security readiness assessment framework at country level. [In:] N. Clarke and S. Furnell (Eds.), *Proceedings of the 18th IFIP WG 11.12 International Symposium "Human Aspects of Information Security and Assurance"*, pp. 93–106, Cham: Springer, https://doi.org/10.1007/978-3-031-72559-3_7.

Alghassab, M. 2022. Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector. *Energies* 15(1), https://doi.org/10.3390/en15010218.

Ampratwum et al. 2023 – Ampratwum, G., Tam, V.W.Y. and Osei-Kyei, R. 2023. Critical analysis of risks factors in using public-private partnership in building critical infrastructure resilience: A systematic review. *Construction Innovation* 23(2), pp. 360–382, https://doi.org/10.1108/CI-10-2021-0182.

Anguelov, K. and Kavaldzhieva, K. 2021. Methodology for determining the socio-economic factors in the performance of Cost-Benefit Analysis for the production of electricity from biomass. [In:] *2021 17th Conference on Electrical Machines, Drives and Power Systems, ELMA 2021 – Proceedings*. Sofia: Institute of Electrical and Electronics Engineers, https://doi.org/10.1109/ELMA52514.2021.9502978.

Annual analytical review (October 2023–September 2024) 2024. [Online:] https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf [Accessed: 2026-01-15].

Assante, M. 2016. *Confirmation of a coordinated attack on the Ukrainian power grid*. [Online:] https://www.readkong.com/page/analysis-of-the-cyber-attack-on-the-ukrainian-power-grid-6826988 [Accessed: 2026-01-15].

Biluk et al. 2020 – Biluk, I., Shareyko, D., Fomenko, A., Havrylov, S., Savchenko, O. and Hruban, V. 2020. Adaptive Control in Complete Electric Drives. [In:] *Proceedings of the 25th IEEE International Conference on Problems of Automated Electric Drive. Theory and Practice, PAEP 2020*, Kremenchuk: Institute of Electrical and Electronics Engineers, https://doi.org/10.1109/PAEP49887.2020.9240856.

Boiko et al. 2023 – Boiko, S., Kasatkina, I. and Danilin, O. 2023. Aspects of reconfiguration of electrical supply systems when implementing distributed generation sources in the terms of distribution networks of enterprises. *Journal of Kryvyi Rih National University* 21(1), pp. 169–174, https://doi.org/10.31721/2306-5451-2023-1-56-169-174.

Brunet-Jailly, E. 2022. Cross-border cooperation: A global overview. *Alternatives* 47(1), pp. 3–17, https://doi.org/10.1177/03043754211073463.

Carrapico, H. and Farrand, B. 2024. Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *Journal of Common Market Studies* 62(S1), pp. 147–158, https://doi.org/10.1111/jcms.13654.

Casino et al. 2022 – Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A. and Patsakis, C. 2022. SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity* 8(1), https://doi.org/10.1093/cybsec/tyac014.

Code of Ukraine "On Administrative Offences" 1984. [Online:] https://zakon.rada.gov.ua/laws/show/80731-10?lang=en#Text [Accessed: 2026-01-15].

Convention on Cybercrime (ETS No. 185) 2001. [Online:] https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-cybercrime-ets-no-185-translations [Accessed: 2026-01-15].

Criminal Code of Ukraine 2001. [Online:] https://zakon.rada.gov.ua/laws/show/2341-14?lang=en#Text [Accessed: 2026-01-15].

Cyber Resilience Act 2025. [Online:] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act [Accessed: 2026-01-15].

Dai et al. 2025 – Dai, Z.C., Tan, M., Yang, Y., Liu, X., Wang, R. and Su, Y.X. 2025. Massive Coordination of Distributed Energy Resources in VPP: A Mean Field RL-Based Bi-Level Optimization Approach. *IEEE Transactions on Cybernetics*, https://doi.org/10.1109/TCYB.2024.3525121.

Danchuk, V. and Danchuk, M. 2024. Integration of blockchain technologies into cybersecurity systems for critical infrastructure facilities: Prospects and challenges. *Bulletin of Cherkasy State Technological University* 29(4), pp. 43–52, https://doi.org/10.62660/bcstu/4.2024.43.

Decree of the President of Ukraine No. 242/2016 "On the National Coordination Centre for Cybersecurity" 2021. [Online:] https://zakon.rada.gov.ua/laws/show/242/2016?lang=en#Text [Accessed: 2026-01-15].

Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 'On the Cybersecurity Strategy of Ukraine'" 2021. [Online:] https://www.president.gov.ua/documents/4472021-40013 [Accessed: 2026-01-15].

Directive (EU) No. 2022/2555 of the European Parliament and of the Council "On Measures for a High Common Level of Cybersecurity Across the Union" 2022. [Online:] http://data.europa.eu/eli/dir/2022/2555/oj [Accessed: 2026-01-15].

Dong et al. 2022 – Dong, S., Cao, J., Flynn, D. and Fan, Z. 2022. Cybersecurity in smart local energy systems: Requirements, challenges, and standards. *Energy Informatics* 5, 9, https://doi.org/10.1186/s42162-022-00195-7.

eIDAS Regulation 2025. [Online:] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation [Accessed: 2026-01-15].

EU supports cybersecurity in Ukraine with over 10 million euro 2022. [Online:] https://www.eeas.europa.eu/delegations/ukraine/eu-supports-cybersecurity-ukraine-over-10-million-euro_en?s=232 [Accessed: 2026-01-15].

EU4DigitalUA 2025. [Online:] https://eu4digitalua.eu/en/about-en/ [Accessed: 2026-01-15].

European Resource Adequacy Assessment 2022 Edition 2022. [Online:] https://www.entsoe.eu/outlooks/eraa/2022/ [Accessed: 2026-01-15].

Firoozjaei et al. 2022 – Firoozjaei, M.D., Mahmoudyar, N., Baseri, Y. and Ghorbani, A.A. 2022. An evaluation framework for industrial control system cyber incidents. *International Journal of Critical Infrastructure Protection* 36, https://doi.org/10.1016/j.ijcip.2021.100487.

Fornusek, M. 2024. *SBU has repelled almost 10,000 cyberattacks since 2022*. [Online:] https://kyivindependent.com/sbu-cuts-supply-of-components-for-russian-drones-missiles/ [Accessed: 2026-01-15].

Hrynchyshyna, V. 2024. Information technology in the context of international relations: Cybersecurity as one of the challenges of the modern digital age. Kyiv: National University of "Kyiv-Mohyla Academy".

Işık et al. 2025a – Işık, C., Ongan, S., Islam, H., Yan, J., Alvarado, R. and Ahmad, M. 2025. The nexus of economic growth, energy prices, climate policy uncertainty (CPU), and digitalization on ESG performance in the USA. *Climate Services* 38, https://doi.org/10.1016/j.cliser.2025.100572.

Işık et al. 2025b – Işık, C., Yan, J. and Ongan, S. 2025. Energy intensity, supply chain digitization, technological progress bias in China's industrial sectors. *Energy Economics* 145, https://doi.org/10.1016/j.eneco.2025.108442.

Khan, S. and Madnick, S. 2021. Cybersafety: A system-theoretic approach to identify cyber-vulnerabilities and mitigation requirements in industrial control systems. *IEEE Transactions on Dependable and Secure Computing* 19(5), pp. 3312–3328, https://doi.org/10.1109/TDSC.2021.3093214.

Korosteleva, J. 2022. The implications of Russia's invasion of Ukraine for the EU energy market and businesses. *British Journal of Management* 33(4), pp. 1678–1682, https://doi.org/10.1111/1467-8551.12654.

Kravchuk et al. 2024 – Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T. and Ukhach, V. 2024. Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security* 2(2), pp. 28–38, https://doi.org/10.62566/lps/2.2024.28.

Krechko, O. and Mikhaylov, A. 2025. Global electricity generation from renewable sources using fuzzy sets and spatial analysis: revolution in solar and wind energy in BRICS countries. *Quality and Quantity* 59(2), pp. 1553–1571, https://doi.org/10.1007/s11135-024-02033-2.

Krimmer et al. 2021 – Krimmer, R., Dedovic, S., Schmidt, C. and Corici, A.A. 2021. Developing cross-border e-Governance: Exploring interoperability and cross-border integration. [In:] N. Edelmann et al. (Eds.), *Proceedings of the 13th IFIP WG 8.5 International Conference "Electronic Participation"*, pp. 107–124, Cham: Springer, https://doi.org/10.1007/978-3-030-82824-0_9.

Krykun, V.V. 2022. Corruption risks of the Law of Ukraine "On critical infrastructure". *Scientific Bulletin of Dnipropetrovsk State University 'Actual Problems of Domestic Jurisprudence'* 6, pp. 141–146, https://doi.org/10.32782/39221400.

Kuniev, Y.D. and Krutas, V.O. 2021. Administrative regulation of offences in the information sphere. [In:] *Proceedings of the XI International Scientific and Practical Conference "Modern Law in the Era of Social Change"*, pp. 181–183. Kyiv: National Aviation University.

Kuznietsova et al. 2022 – Kuznietsova, O., Yastremska, L., Korniyenko, I. and Baranovskyy, M. 2022. Environmental orientation of energy policy of the EU and Ukraine. *Technologies and Engineering* 23(4), pp. 17–34, https://doi.org/10.30857/2786-5371.2022.4.2.

Law of Ukraine No. 1366-IX "On Amendments to the Code of Ukraine on Administrative Offences and the Criminal Code of Ukraine on Strengthening Liability for Violation of Fire and Technological Safety Requirements" 2021. [Online:] https://zakon.rada.gov.ua/laws/show/en/1366-20?lang=en#Text [Accessed: 2026-01-15].

Law of Ukraine No. 1882-IX "On Critical Infrastructure" 2021. [Online:] https://zakon.rada.gov.ua/laws/show/1882-20?lang=en#Text [Accessed: 2026-01-15].

Law of Ukraine No. 2019-VIII "On Electricity Market" 2017. [Online:] https://zakon.rada.gov.ua/laws/show/2019-19?lang=en#Text [Accessed: 2026-01-15].

Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine" 2017. [Online:] https://zakon.rada.gov.ua/laws/show/2163-19/ed20240628?lang=en#Text [Accessed: 2026-01-15].

Law of Ukraine No. 2229-XII "On Security Service of Ukraine" 1992. [Online:] https://zakon.rada.gov.ua/laws/show/2229-12?lang=en#Text [Accessed: 2026-01-15].

Law of Ukraine No. 222-VIII "On Licensing of Economic Activity Types" 2015. [Online:] https://zakon.rada.gov.ua/laws/show/222-19?lang=en#Text [Accessed: 2026-01-15].

Law of Ukraine No. 2297-VI "On Protection of Personal Data" 2010. [Online:] https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text [Accessed: 2026-01-15].

Law of Ukraine No. 3855-XII "On State Secret" 1994. [Online:] https://zakon.rada.gov.ua/laws/show/3855-12?lang=en#Text [Accessed: 2026-01-15].

Law of Ukraine No. 80/94-VR "On Protection of Information in Automated Systems" 1994. [Online:] https://zakon.rada.gov.ua/laws/show/en/80/94-%D0%B2%D1%80?lang=en#Text [Accessed: 2026-01-15].

Lella et al. 2023 – Lella, I., Tsekmezoglou, E., Theocharidou, M., Magonara, E., Malatras, A., Svetozarov Naydenov, R. and Ciobanu, C. 2023. *ENISA Threat Landscape*. https://doi.org/10.2824/782573.

Li, X. and Tian, G. 2024. Analyzing Internet Finance Model Using Big Data Financial Intermediation. *Journal of Engineering Project and Production Management* 14(1), https://doi.org/10.32738/JEPPM-2024-0008.

Liebetrau, T. 2024. Problematising EU cybersecurity: Exploring how the single market functions as a security practice. *Journal of Common Market Studies* 62(3), pp. 705–724, https://doi.org/10.1111/jcms.13523.

Malatji et al. 2022 – Malatji, M., Marnewick, A.L. and Von Solms, S. 2022. Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security* 30(2), pp. 255–279, https://doi.org/10.1108/ICS-06-2021-0091.

Markopoulou et al. 2019 – Markopoulou, D., Papakonstantinou, V. and de Hert, P. 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review* 35(6), https://doi.org/10.1016/j.clsr.2019.06.007.

Odebade, A.T. and Benkhelifa, E. 2023. A comparative study of national cyber security strategies of ten nations. *arXiv* 2303. https://doi.org/10.48550/arXiv.2303.13938.

On sharing information on cyber threats 2022. [Online:] https://cert.gov.ua/article/39962 [Accessed: 2026-01-15].

Onykiienko, Yu. and Mazin, M. 2025. Application of wavelet transformations on microcontrollers for monitoring and optimising energy systems in industrial conditions. *Journal of Kryvyi Rih National University* 23(1), pp. 56–67, https://doi.org/10.31721/2306-5451-2025-1-23-56-67.

Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine No. 93 "On Approval of the Regulation on State Expertise in the Field of Technical Information Protection" 2007. [Online:] https://zakon.rada.gov.ua/laws/show/en/z0820-07?lang=en#Text [Accessed: 2026-01-15].

Order of the Administration of the State Service of Special Communications and Information Protection of Ukraine No. 1009 "On Approval of the Annual Plan for Implementation of State Supervision (Control) Measures in the Field of Compliance with Legislative Requirements for the Provision of Services in the Field of Technical Information Protection and Cryptographic Information Protection (Except for Electronic Trust Services) by the Administration of the State Service of Special Communications and Information Protection of Ukraine for 2024" 2023. [Online:] https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-01-grudnya-2023-roku-1009-pro-zatverdzhennya-richnogo-

planu-zdiisnennya-zakhodiv-derzhavnogo-naglyadu-kontrolyu-u-sferi-doderzhannya-vimog-zakonodavstva-z-nadannya-poslug-u-galuzi-tekhnichnogo-zakhistu-informaciyi-ta-kriptografichnogo-zakhistu-informaciyi-krim-elektronnikh-dovirchikh-poslug-administraciyeyu-derzhavnoyi-sluzhbi-specialnogo-zv-yazku-ta-zakhistu-informaciyi-ukrayini-na-2024-rik [Accessed: 2026-01-15].

Order of the Cabinet of Ministers of Ukraine No. 1351-p "On Approval of the Strategy for Digital Development of Innovation Activities of Ukraine for the Period Up to 2030 and Approval of the Operational Action Plan for Its Implementation in 2025–2027" 2024. [Online:] https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text [Accessed: 2026-01-15].

Osička, J. and Černoch, F. 2022. European energy politics after Ukraine: The road ahead. *Energy Research & Social Science* 91, https://doi.org/10.1016/j.erss.2022.102757.

Parkes et al. 2024 – Parkes, J., Chan, D., Chan, S.Y. and Enobun, W. 2024. *ISC census and annual report*. [Online:] https://www.isc.co.uk/media/uukn4r3i/isc_census_2024_15may24.pdf [Accessed: 2026-01-15].

Pollini et al. 2022 – Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. and Guerri, D. 2022. Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work* 24, pp. 371–390, https://doi.org/10.1007/s10111-021-00683-y.

Rajkumar et al. 2023 – Rajkumar, V.S., Ştefanov, A., Presekal, A., Palensky, P. and Torres, J.L.R. 2023. Cyber attacks on power grids: Causes and propagation of cascading failures. *IEEE Access* 11, pp. 103154–103176, https://doi.org/10.1109/ACCESS.2023.3317695.

Regulation (EU) No. 2019/943 of the European Parliament and of the Council "On the Internal Market for Electricity" 2019. [Online:] http://data.europa.eu/eli/reg/2019/943/2024-07-16 [Accessed: 2026-01-15].

Relations with Ukraine 2025. [Online:] https://www.nato.int/cps/uk/natohq/topics_37750.htm?selectedLocale=en [Accessed: 2026-01-15].

Resolution of the Board of the National Bank of Ukraine No. 178 "On Approval of the Regulation on Organisation of Cyber Defence in the Banking System of Ukraine and Amendments to the Regulation on Determination of Critical Infrastructure Objects in the Banking System of Ukraine" 2022. [Online:] https://zakon.rada.gov.ua/laws/show/v0178500-22?lang=en#Text [Accessed: 2026-01-15].

Resolution of the Cabinet of Ministers of Ukraine No. 444 "On Approval of the Procedure for Training the Population to Act in Emergency Situations" 2013. [Online:] https://zakon.rada.gov.ua/laws/show/444-2013-%D0%BF?lang=en#Text [Accessed: 2026-01-15].

Safeguarding cyberspace together: SSSCIP, NCCC, and ENISA sign working arrangement 2023. [Online:] https://cip.gov.ua/en/news/razom-na-zakhisti-kiberprostoru-derzhspeczv-yazku-nkck-ta-enisa-pidpisali-ugodu-pro-spivpracyu [Accessed: 2026-01-15].

Savchuk, S.O. 2024. Challenges and opportunities of integration of Ukraine in the EU cyber security system. *Economics, Management and Administration* 108(2), pp. 198–203, https://doi.org/10.26642/ema-2024-2(108)-198-203.

Semenenko et al. 2024 – Semenenko, O., Onofriichuk, V., Tolok, P., Rieznik, V. and Momot, D. 2024. Analysis of Ukraine's external military-economic relations during the war with Russia. *Scientific Bulletin of Mukachevo State University. Series "Economics"* 11(1), pp. 71–82, https://doi.org/10.52566/msu-econ1.2024.71.

Singh, C. 2023. The European approach to cybersecurity in 2023: A review of the changes brought in by the network and information security 2 (NIS2) Directive 2022/2555. *International Company and Commercial Law Review* 5, pp. 251–261.

Striolo, A. and Huang, S. 2022. Upcoming transformations in integrated energy/chemicals sectors: Some challenges and several opportunities. *The Journal of Physical Chemistry C* 126(51), pp. 21527–21541, https://doi.org/10.1021/acs.jpcc.2c05192.

Sulich et al. 2021 – Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J. and Zema, T. 2021. Cybersecurity and sustainable development. *Procedia Computer Science* 192, pp. 20–28, https://doi.org/10.1016/j.procs.2021.08.003.

Tanasiichuk et al. 2024 – Tanasiichuk, A., Tyukhtenko, N., Zaburmekha, Y., Sokoliuk, S., Prokopchuk, O., Krupskyi, A. and Tsurkanov, M. 2024. Sustainable Development Strategy of Enterprises in International Markets: Opportunities and Challenges. *European Journal of Sustainable Development* 13(3), pp. 311–328, https://doi.org/10.14207/ejsd.2024.v13n3p311.

The European Union supports Ukraine's digital transformation: Results of EU4DigitalUA's work 2024. [Online:] https://www.eeas.europa.eu/delegations/ukraine/european-union-supports-ukraines-digital-transformation-results-eu4digitaluas-work_en?page_lang=en&s=232 [Accessed: 2026-01-15].

The vulnerability detection and cyber incidents/cyber attacks response system helped to detect and process 1,042 cyber incidents in 2024, 2025. [Online:] https://scpc.gov.ua/en/articles/383 [Accessed: 2026-01-15].

Tsybka, A.A. 2025. Administrative and legal measures to address threats to energy security in the electricity and nuclear energy sectors. *Kyiv Law Journal* 4, pp. 101–109, https://doi.org/10.32782/klj/2024.4.14.

Ukraine–U.S. cooperation in cybersecurity area reaches a new level 2022. [Online:] https://cip.gov.ua/en/news/ukrayino-amerikanske-spivrobitnictvo-u-sferi-kiberbezpeki-vikhodit-na-novii-riven [Accessed: 2026-01-15].

Umair, M. and Guliyeva, S. 2025. Optimizing welfare and market power: Energy storage strategies in renewable-integrated power markets. *Journal of Energy Storage* 118, https://doi.org/10.1016/j.est.2025.116315.

Weber, C. 2023. Achievements and challenges in European energy markets. *Journal of Modern Power Systems and Clean Energy* 11(3), pp. 698–704, https://doi.org/10.35833/MPCE.2023.000061.

Yasenenko, V. 2025. Cyber defence automation: Can AI outperform hackers? *Technologies and Engineering* 26(3), pp. 89–99, https://doi.org/10.30857/2786-5371.2025.3.7.

Yevdokymov, S. 2025. Mathematical modelling and neural networks in the context of railway cybersecurity. *Information Technologies and Computer Engineering* 22(2), pp. 107–117, https://doi.org/10.31649/vitce/2.2025.107.

Zaikina, H.M. 2024. Some issues of administrative and legal support of cybersecurity: The experience of the USA and the EU. In: *Proceedings of the XII International Scientific and Practical Conference "Human, Society, Communication Technologies"*, pp. 131–133, Kharkiv: Ukrainian State University of Railway Transport.

Zografopoulos et al. 2023 – Zografopoulos, I., Hatziargyriou, N.D. and Konstantinou, C. 2023. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. *IEEE Systems Journal* 17(4), pp. 6695–6709, https://doi.org/10.1109/JSYST.2023.3305757.

Viacheslav Politanskyi, Hanna Zaikina, Yuliia Mekh, Volodymyr Martynovskyi,
Liliia Pyliuha

Cyberbezpieczeństwo sektora energetycznego Ukrainy: mechanizmy administracyjne i prawne ochrony infrastruktury krytycznej państwa

Streszczenie

Celem badania było zbadanie aktualnego stanu, skuteczności i wyzwań w funkcjonowaniu mechanizmów administracyjnych i prawnych zapewniających cyberbezpieczeństwo w sektorze energetycznym Ukrainy w warunkach wzmożonych zagrożeń. Metodologia pracy obejmowała zastosowanie metod teoretycznych, w szczególności formalnoprawnej analizy ustawodawstwa ukraińskiego i aktów międzynarodowych, metody prawnoporównawczej (porównanie z praktyką Unii Europejskiej, Stanów Zjednoczonych Ameryki i Izraela), analizy systemowej interakcji instytucjonalnych (Państwowa Służba Łączności Specjalnej i Ochrony Informacji Ukrainy, Narodowe Centrum Koordynacji Cyberbezpieczeństwa) oraz analizy oficjalnych raportów. Stwierdzono, że pomimo istnienia podstawowych ram regulacyjnych i instytucjonalnych, ich praktyczne wdrożenie napotkało znaczne trudności. Zidentyfikowano istotne luki we wdrażaniu wymogów cyberbezpieczeństwa przez operatorów obiektów energetycznych, niedostateczne uszczegółowienie regulacji dotyczących zautomatyzowanych systemów sterowania procesami i bezpieczeństwa przemysłowych systemów sterowania, problemy z efektywnością kontroli państwowej wynikające z ograniczonych zasobów oraz potrzebę dogłębnej wiedzy technicznej. Współpraca międzynarodowa i harmonizacja z normami europejskimi zostały uznane za istotne czynniki wzmacniające odporność, chociaż wdrożenie wymagało spójności. Wyniki badania i przedstawione rekomendacje (dotyczące opracowania standardów sektorowych, wzmocnienia nadzoru, wsparcia operatorów i rozwoju zasobów ludzkich) mogłyby zostać wykorzystane przez organy publiczne do ulepszenia przepisów i praktyki administracyjnej w celu zwiększenia cyberodporności krytycznej infrastruktury energetycznej.

Słowa kluczowe: orzecznictwo, globalna cyfryzacja, technologie operacyjne, standardy międzynarodowe, przemysłowe systemy sterowania, reagowanie na incydenty, współpraca międzynarodowa