UDC 004.056:005.591.6(477)
DOI: 10.32518/sals1.2025.70

Соціально-правові студії. 2025. Т. 8, № 1
Social & Legal Studios. 2025. Vol. 8, No. 1

Ways to improve legal regulation of critical infrastructure information networks protection

Oleksandr Holovko*

PhD in Public Administration
National Academy of the Security Service of Ukraine
03066, 22 Mykhailo Maksymovych Str., Kyiv, Ukraine
https://orcid.org/0009-0004-9576-7737

Olena Kravchenko

PhD in Law, Head of Science Laboratory
National Academy of the Security Service of Ukraine
03066, 22 Mykhailo Maksymovych Str., Kyiv, Ukraine
https://orcid.org/0000-0003-0246-1022

Mykola Pogrebytskyi

Doctor of Law, Professor
National Academy of the Security Service of Ukraine
03066, 22 Mykhailo Maksymovych Str., Kyiv, Ukraine
https://orcid.org/0000-0003-0779-6577

Ivan Romaniuk

PhD in Law
National Academy of the Security Service of Ukraine
03066, 22 Mykhailo Maksymovych Str., Kyiv, Ukraine
https://orcid.org/0000-0003-4788-8046

Abstract. The study aimed to identify ways to improve the legal regulation of the protection of information networks of Ukraine's critical infrastructure, taking into account contemporary challenges in cybersecurity and international standards. The research employed a comparative analysis of the legislation of Ukraine, the EU, the USA, and the United Kingdom governing cybersecurity in critical infrastructure. Additionally, it assesses the effectiveness of existing legal and regulatory frameworks in the context of modern threats, particularly armed conflict. The analysis revealed the fragmented nature of the current legislation, the lack of an effective coordination mechanism among state authorities, and insufficient legal instruments for regulating liability for cybercrimes targeting critical infrastructure. It was established that Ukraine's regulatory framework only partially complies with international standards, complicating its harmonisation with EU requirements. The insufficient integration of the public and private sectors in the field of cybersecurity is also a significant factor limiting the effectiveness of protecting strategic digital assets. To enhance the efficiency of legal regulation, comprehensive harmonisation of Ukraine's legislation with EU norms is necessary, particularly with the NIS 2 Directive, which establishes unified requirements for the protection of critical infrastructure. The introduction of mandatory certification of cybersecurity measures and the expansion of criminal liability for cyberattacks on critical infrastructure, including sanctions for legal entities, are advisable. A crucial direction is the legislative establishment of a unified national cyber threat monitoring system and the improvement of mechanisms for public-private partnerships. The proposed changes will contribute to strengthening the cyber resilience of Ukraine's critical infrastructure, ensuring its compliance with international standards, and facilitating its integration into the global cybersecurity system

Keywords: cyber resilience; digital space; strategic objects; cyber threats; national security

Suggested Citation **Article's History**: Received: 17.09.2024 Revised: 07.02.2025 Accepted: 26.03.2025

Holovko, O., Kravchenko, O., Pogrebytskyi, M., & Romaniuk, I. (2025). Ways to improve legal regulation of critical infrastructure information networks protection. *Social & Legal Studios*, 8(1), 70-81. doi: 10.32518/sals1.2025.70.

*Corresponding author

Introduction

In the contemporary digital era, cyber threats to vital infrastructure have evolved into a global concern that transcends national boundaries. Advanced cyberattacks aimed at energy, transportation, communication, and healthcare systems represent a mounting threat to governments, businesses, and critical service providers worldwide. These vulnerabilities underscore the pressing need for comprehensive cybersecurity strategies that encompass organisational, legal, and technological safeguards. The accelerated integration of digital technologies and the interconnection of global economies have elevated the protection of critical infrastructure to a paramount concern in national security strategies across diverse geographical regions.

To address the challenges posed by contemporary cybersecurity, a multifaceted approach encompassing organisational, legal, and cyber-physical methodologies is imperative. Recent research contributions offer significant insights into the evolution of cybersecurity. In particular, Ü. Cali *et al.* (2023) emphasise the need to integrate physical and cyber security measures to enhance the resilience of digital water infrastructure against cyber threats, and A. Semenchenko *et al.* (2020) highlight the necessity of comprehensive cyber-physical solutions to mitigate the impact of cyberattacks on critical utilities. The authors draw attention to the legal system's fragmentation and the necessity of governmental entities working together more closely. The growth of cybersecurity regulations inside the European Union is also examined by G.G. Fuster and L. Jasmontaite (2020), who emphasise the significance of striking a balance between security concerns and basic rights. The authors contend that a unified strategy including several domains, such as critical infrastructure protection and electronic communications, is necessary for efficient cybersecurity governance.

R. Kelemen (2023) has conducted an in-depth analysis of the repercussions of the Russian-Ukrainian war on European cybersecurity policies, with a particular focus on the impact of hybrid warfare on cybersecurity strategies. The study asserts the necessity for a paradigm shift towards integrated cybersecurity frameworks that encompass both cognitive and digital security measures. Additionally, I. Shopina *et al.* (2020) have undertaken a comparative analysis of the organisational and legislative cybersecurity strategies employed by the EU, NATO, and leading nations. In order to enhance resilience against cyber threats, their analysis underscores the imperative for Ukraine to integrate its cybersecurity framework with international norms.

H. Zhang *et al.* (2024) examine the function of Continuous Auditing (CA) in the War Potential Network (WPN), a pivotal infrastructure architecture impacting national security. The study underscores the challenges in ensuring compliance with privacy laws and national security regulations, emphasising the need for advanced auditing techniques such as Locality-Sensitive Hashing (LSH). The research provides novel insights on defending vital infrastructures from cyberattacks while upholding moral and legal principles through the integration of compliance-enhancing technologies. In a related study, D. Markopoulou and V. Papakonstantinou (2021) examine the evolution of critical infrastructure protection, with a particular focus on the EU. In order to detect legislative gaps that affect cybersecurity measures, their research distinguishes between critical infrastructures and critical information infrastructures. They illustrate how the growing frequency of cyber events calls for enhanced regulatory frameworks and sector-specific protective mechanisms in order to adjust to the digital age, using the healthcare industry as a case study.

Despite numerous papers, a number of elements of the problem under study require more detailed analysis. The issues of assessing the vulnerabilities of information networks of critical state resources of Ukraine, the effectiveness of existing mechanisms for their protection, the formation of innovative methodologies for ensuring cyber resilience of critical objects, and considering the features of hybrid threats, require further investigation.

The purpose of the study was to examine ways to improve the legal regulation of critical infrastructure information network protection. The following tasks were set:

1) analyse modern approaches to the legal regulation of critical infrastructure protection and categorisation of critical infrastructure objects.

2) investigate the effectiveness of existing cybersecurity frameworks and policies in protecting critical infrastructure information networks.

3) develop proposals for improving regulatory frameworks to enhance the security of information networks in Ukraine.

Materials and methods

The research methodology provided an interdisciplinary approach that combined a variety of scientific research methods and a wide range of data. A comprehensive analysis of information networks of strategically important objects as a complex system functioning in the face of external threats was conducted. This allowed identifying the relationships between different components of the system and assessing the impact of various factors on its vulnerability and sustainability. The comparative legal method was used to compare regulatory legal acts and practices of critical infrastructure protection in Ukraine and other countries, in particular, the United States (Cybersecurity and Infrastructure..., 2018), Great Britain (the Network and..., 2018), and Germany (Act on the..., 2009). This helped to identify common features and differences in approaches to regulating and protecting critical infrastructure and evaluate the effectiveness of diverse cybersecurity models. Chronological analysis was used to track the transformation of approaches to protecting strategically important objects and analyse previous cyber incidents related to attacks on critical infrastructure. This contributed to the examination of cyberattack methods and appropriate defence mechanisms. Analytical materials of international organisations (Cloud consciousness: Industry..., 2015) and the NotPetya cyberattack in 2017 (The history of..., 2018) were used to assess the consequences of large-scale cyber incidents and identify weaknesses in existing security measures.

The research materials were regulatory legal acts of Ukraine in the field of cybersecurity and critical infrastructure protection, in particular, Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), Law of Ukraine 1882-IX "On Critical Infrastructure" (2023), Cybersecurity Strategy of Ukraine (Decree of the..., 2021), National Security Strategy of Ukraine (Decree of the..., 2020), Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p "On Approval of the General

Requirements for Cyber Defence of Critical Infrastructure Objects" (2019), Criminal Code of Ukraine (2001), in particular, articles related to cybercrime.

Results

Analysis of the state of protection of information networks of critical infrastructure of Ukraine in 2014-2024. The key document in this area is the Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017). This Regulatory Act outlines the legal and structural principles for ensuring the key needs of an individual and society, community, and country in a digital environment. However, experts note that the existing regulatory framework needs further improvement, in particular, against the background of rapid progress in innovation and new challenges associated with military aggression. P. Anakhov *et al.* (2023) posit that Ukraine's current cybersecurity legislation is inadequate in addressing the escalating complexity of cyber threats within the context of armed conflict, underscoring the necessity for a comprehensive overhaul of regulatory mechanisms. In a similar vein, A. Davydiuk and V. Zubok (2023) emphasise that while legal frameworks provide a foundation for cybersecurity, their practical implementation remains inconsistent due to inadequate coordination between state agencies. In a similar vein, R. Chernysh *et al.* (2023) underscore the pressing need to align Ukraine's cybersecurity strategies with international standards to bolster resilience against state-sponsored cyber threats.

The institutional structure of ensuring cybersecurity in Ukraine includes a number of state bodies. Their activities are coordinated by the National Cybersecurity Coordination Centre under the National Security and Defence Council of Ukraine (NSDC) (Decree of the President of Ukraine No. 242/2016, 2016). However, the effectiveness of interaction between these structures often faces challenges related to the distribution of powers, which can negatively affect the speed of response to cyber threats. Technical means of critical infrastructure information networks preventive measures demonstrate a heterogeneous level of development. Some sectors, such as banking and energy, have relatively advanced cyber defence systems. However, many critical infrastructure facilities, especially in the regions, still use outdated technologies and software, making them vulnerable to modern cyber threats (The history of..., 2018). The situation is compounded by limited funding and a shortage of cybersecurity professionals, especially in the public sector.

Regarding cybersecurity strategies of Ukraine, 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) defines key priorities in the field of cyber defence, including the development of the national cybersecurity system, strengthening the capabilities of security and defence sector entities to effectively counter cyber threats, and ensuring the cyber resilience of critical infrastructure. An important aspect of the strategy is the focus on the development of public-private partnership and international cooperation in the field of cybersecurity. The document also provides for the creation of a system of training personnel in the field of cybersecurity, which is critical to overcoming the shortage of qualified specialists in this field. The cybersecurity strategy of Ukraine defines critical priorities in the field of cyber defence, including the development of a national cybersecurity system, strengthening the capabilities of security and defence sector entities to effectively counter cyber threats, as well as ensuring the cyber resilience of critical infrastructure (Shahini *et al.*, 2024). The document provides for the creation of a system of training personnel in the field of cybersecurity and focuses on the development of public-private partnership and international cooperation. These provisions of the strategy correspond to the needs identified in the course of the study to strengthen the protection of information networks of critical infrastructure in Ukraine.

In the field of public-private partnership, Ukraine is substantially inferior to the advanced states of the world. In the United States, the Critical Infrastructure Partnership Advisory Council (2023) programme operates, which ensures effective interaction between the government apparatus and entrepreneurship in the field of critical infrastructure preventive measures. In Ukraine, such mechanisms are just beginning to take shape, which limits the opportunities for information exchange and coordination between public authorities and private operators of critical infrastructure. Regarding the standardisation and certification of preventive measures systems, Ukraine is in the process of adapting international standards, such as the International Organisation for Standardisation (ISO) and the National Institute of Standards and Technology (NIST). However, the level of implementation of these standards at critical infrastructure facilities remains insufficient. According to the State Service for Special Communications and Information Protection of Ukraine, only about 30% of critical infrastructure facilities fully comply with international cybersecurity standards, which is substantially lower than the levels of EU states and the US (Key Consequences of..., 2022).

The issue of personnel support requires exceptional focus. There is an acute shortage of cybersecurity specialists in Ukraine, especially in the public sector. The need for such specialists is met only by 50-60%. For comparison, in the EU countries, this figure is 80-85%. This creates substantial security risks for critical infrastructure, especially in the context of steadily expanding the scope and complicating cyber-attacks. Analysing the regulatory support for the preservation of information networks of critical infrastructure in Ukraine, it is worth paying attention to its evolution and compliance with modern challenges. The Law of Ukraine No. 1882-IX "On Critical Infrastructure" (2023) was an important step in the formation of an integrated approach to the protection of critical objects. However, the comparative legal analysis indicates the need to continue coordinating national legal norms with EU norms, in particular, with the Directive of the European Parliament and the Council No. 2016/1148 "Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union" (2016).

From the standpoint of the legal consequences of cyber-attacks on critical infrastructure facilities, Ukrainian legislation shows certain gaps (Yefimenko *et al.*, 2023b). Article 361 of the Criminal Code of Ukraine (2001) provides for liability for obstructing the operation of computers, digital complexes, and information infrastructures. However, this rule does not cover the full range of modern cyber threats, such as attacks on industrial Incident Command Systems (ICS) or distributed denial-of-service attacks, which are often used against critical infrastructure objects.

In terms of organisational support, the creation of the national cybersecurity coordination centre under the National Security and Defence Council of Ukraine was an advanced step in coordinating the efforts of various departments (Decree of the President of Ukraine No. 242/2016, 2016). However, the analysis of its activities indicates the need to expand the powers and resources provided for the effective performance of the tasks assigned to it. In particular, the issue of creating a unified system for monitoring, recognising and countering digital violations, similar to the United States Computer Emergency Readiness Team in the United States or the Computer Emergency Response Team in the EU, remains relevant. Regarding the regulation of the protection of information networks of critical infrastructure in Ukraine, special attention should be paid to the implementation of international standards and norms. In particular, the Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017) provides for the application of international ISO standards and other standards on information and cybersecurity. However, the analysis of the regulatory framework indicates a lack of detail in the mechanisms for implementing these standards and clear criteria for assessing their compliance.

The key issue is the regulatory regulation of the cross-border exchange of information about cyber incidents. Ukraine is a participant in the Convention on Cybercrime, which creates the legal basis for global cooperation in this area (Law of Ukraine 2824-IV, 2005). However, the practical implementation of the provisions of the convention faces a number of problems, in particular, regarding the speed of data exchange and their admissibility as evidence in court proceedings. From the standpoint of administrative and legal regulation, the role of Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p "On Approval of the General Requirements for Cyber Defence of Critical Infrastructure Objects" (2019) is notable. This Regulatory Act sets basic requirements for threat prevention systems, but expert analysis indicates the need for its further detailing and adaptation to the specific features of various sectors of critical infrastructure.

According to the analytical report of the National Coordination Centre for Cybersecurity, in 2023-2024 there is a substantial increase in the number and complexity of cyber-attacks on critical infrastructure facilities in Ukraine (Critical Infrastructure Partnership, 2023). For an integrated assessment of the existing security mechanisms of information networks of critical infrastructure of Ukraine, a detailed analysis of key aspects was conducted. The analysis identified substantial discrepancies between the current state of Ukraine and international standards, especially in terms of technical support and investment. Only 30% of critical infrastructure facilities in Ukraine fully meet international standards, compared to 80-90% in the EU countries. In addition, investment in cybersecurity in Ukraine accounts for only 0.1% of the gross domestic product (GDP), while in NATO countries this figure reaches 0.3-0.5%. These data highlight the urgent need for an integrated approach to improving the threat prevention system of Ukraine's critical infrastructure, with a special focus on technical modernisation, human resources development, and strengthening international cooperation (Davydiuk & Potii, 2024). Regarding the confidentiality of personal information processed in the information systems of critical infrastructure facilities, Ukrainian legislation demonstrates a certain non-compliance with the requirements of the EU General Data Protection Regulation. In particular, the Law of Ukraine No. 2297-VI "On Personal Data Protection" (2010) does not contain provisions on mandatory notification of data leaks that are critical for critical infrastructure facilities.

Identification of key vulnerabilities and threats in conflict situations. In the sphere of analysing the crucial vulnerabilities and dangers of information networks of critical infrastructure of Ukraine in the context of conflict, it is worth considering the issue from different angles, covering both legal and technical aspects of the problem. From a legal standpoint, the issue of qualifying cyber-attacks on critical infrastructure facilities in an armed conflict requires priority consideration. In the light of the provisions of international humanitarian law, in particular, the Protocol Additional to the Geneva Conventions of 12 August 1949, and related to the Protection of Victims of International Armed Conflicts (Protocol I) (1977), attacks on objects necessary for the survival of the civilian population are prohibited. However, the specifics of cyber-attacks create certain difficulties in applying these rules since it is often difficult to establish a direct link between cyber operations and physical consequences.

The analysis of the legislative framework of Ukraine reveals certain gaps in the regulation of issues related to the protection of critical infrastructure in a hybrid war. The Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), although defines the basic principles of preventing threats to critical information infrastructure, does not contain specific provisions on countering cyber risks in armed conflict. A comparative analysis with the legislation of NATO countries, particularly the United States and Great Britain, demonstrates the need to develop more detailed legal mechanisms for responding to cyber incidents in wartime. A comparative analysis of the legislation of Ukraine with the regulatory legal acts of the United States, Great Britain, and Germany revealed a number of differences in approaches to protecting critical infrastructure. Cybersecurity and Infrastructure Security Agency Act (2018) in the United States provides for the creation of a specialised agency for cybersecurity and infrastructure protection. The Network and Information Systems Regulations (2018) in the UK set strict requirements for operators of basic services regarding reporting on cyber incidents. The Act on the Federal Office for Information Security (BSI Act – BSIG) (2009) in Germany introduces mandatory minimum IT security standards for critical infrastructure operators. These approaches can be used to improve Ukrainian legislation in the field of critical infrastructure protection. From the standpoint of identifying technical vulnerabilities, special attention should be paid to the problem of preventing threats to SCADA systems that are widely used at critical infrastructure facilities. Research conducted by the State Service for Special Communications and Information Threat Prevention of Ukraine has revealed that a substantial part of these systems in Ukraine uses outdated software and has a low level of threat prevention from external interference. In comparison with the practices of the EU countries, where the standard for preventing threats to industrial control systems has been implemented, the level of security of Ukrainian SCADA systems remains insufficient, which creates substantial risks in conditions of active cyber resistance. An analysis of an attempted cyber-attack on Ukrainian water treatment plants in April 2022

revealed critical vulnerabilities in water supply management systems. According to the report of the State Service for Special Communications and Information Protection of Ukraine, the attackers tried to gain unauthorised access to water quality control systems to change its chemical composition (Key Consequences of..., 2022). The incident highlighted the need to strengthen the protection of SCADA systems in the water supply sector, implement multi-level water quality control systems, and conduct regular cybersecurity exercises for critical infrastructure personnel.

In the context of legal assessment of vulnerabilities, the problem of attribution in conflict situations should be substantially emphasised. According to the United Nations Charter (1945), states have the right to self-defence in the event of an armed attack. However, the qualification of a cyberattack as an "armed attack" remains a controversial issue in international law. The Tallinn guide 2.0, in line with international legal standards on cyber activities, suggests treating cyberattacks resulting in substantial destruction or loss of life as the equivalent of an armed attack (Schmitt, 2017). However, this concept has not yet been widely recognised in international practice, which creates legal uncertainty in the context of preventing threats to Ukraine's critical infrastructure.

Cyber-attacks using the NotPetya virus on the financial sector of Ukraine in 2017 revealed large-scale consequences for the country's critical infrastructure. According to the study, the attack affected not only the banking sector but also energy companies, transportation systems and government agencies (The history of..., 2018). It demonstrated the high level of complexity and organisation of cyber threats, emphasising the need to develop comprehensive cyber defence strategies at the national level. In particular, the incident revealed the need to improve data backup systems, implement more stringent cybersecurity protocols, and strengthen cross-industry cooperation in countering cyber threats.

Attacks on satellite communication systems used to manage critical infrastructure facilities pose a particular threat in conflict situations. The KA-SAT incident, which occurred at the start of the aggression against Ukraine, demonstrated the vulnerability of such systems and their critical importance for national security. From a legal standpoint, such attacks can qualify as a violation of the Convention on Cybercrime (2001) and Law of Ukraine 2824-IV "On Rationalisation of the Convention on Cybercrime" (2005), in particular, Article 4, which deals with illegal data interference. However, the effective prosecution of such crimes is complicated by the cross-border nature of attacks and problems with identifying intruders.

Strategies for strengthening the protection of information networks in Ukraine. As part of the development of strategies to strengthen the protection of information networks of critical infrastructure in Ukraine, the implementation of an integrated approach based on the principles of risk-based management and adaptive threat prevention is of paramount importance. According to the Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), it is necessary to create and implement a multi-level threat prevention system that will cover organisational, technical, and regulatory aspects. A critical element of such a strategy should be the creation of a national cybersecurity system that will ensure the coordination of actions of all cybersecurity entities and prompt response to cyber incidents.

Technically, the priority area is the introduction of advanced technologies for threat prevention, in particular, new-generation IDS intrusion detection and prevention systems based on systems self-learning technologies and cybernetics. According to the recommendations of the European Union Agency for Cybersecurity, the priority task should be to ensure the safety of automated production complexes ICS and SCADA systems that are widely used in the energy and water supply sectors (Cloud consciousness: Industry..., 2015). The implementation of the standard for preventing threats to industrial control systems should become a mandatory requirement for all critical infrastructure facilities. In the legal field, it is necessary to coordinate Ukrainian legal norms with EU norms, in particular, with the Directive of the European Parliament and of the Council No. 2016/1148 "Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union" (2016). This will create a single legal space and ensure effective international cooperation in the field of cybersecurity. An important aspect is also the development of public-private partnership mechanisms in the field of preventing threats to critical infrastructure, which will attract additional assets and professional knowledge of the business environment.

Special attention should be paid to the development of human resources in the field of cyber defence. According to the cybersecurity strategy of Ukraine, approved by 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), it is necessary to create a system for training cybersecurity specialists for the needs of the public sector and critical infrastructure facilities. This includes the development of specialised training programmes, regular trainings on cybersecurity, as well as the creation of a certification system for specialists in accordance with international standards such as ISO/IEC and Certified Information Systems Security Professional. A comprehensive strategy has been developed to systematise and prioritise areas for improving the critical infrastructure threat prevention system in Ukraine. This strategy covers a wide range of activities – from regulatory support to raising staff awareness and considers both technical and organisational aspects of cybersecurity. Special attention is paid to the issues of coordination of Ukrainian legal acts with EU standards, technological modernisation of threat prevention systems, and human resources development. Notably, the implementation of this strategy requires a comprehensive strategy and coordination of efforts of all participants – from public authorities to private operators of critical infrastructure.

Regarding the regulatory support of critical infrastructure, special attention should be paid to the implementation of the provisions of the NIS 2 Directive (2024) in the national legislation of Ukraine. This implementation involves not only the nominal approval of relevant legislative acts but also the creation of effective mechanisms for their implementation. In particular, it is important to create and launch a mechanism for identifying and categorising basic service operators and digital service providers in accordance with the criteria established in the NIS 2 Directive (2024). An important aspect of legal regulation is also the establishment of clear requirements for critical infrastructure operators to implement an Information

Security Management System according to the international ISO standard. Thereby, it is necessary to ensure a differentiated approach to different categories of critical infrastructure objects, considering their specifics and level of criticality. This approach will optimise the cost of ensuring the prevention of threats to the digital space and increase the effectiveness of protective measures.

Special attention should be paid to the issue of critical infrastructure for the dissemination of data on cyber incidents and cyber threats between critical infrastructure operators, government agencies, and international partners. It is necessary to develop and implement regulatory tools that would ensure a balance between the need for rapid exchange of information and the protection of confidential data of business entities. This may include creating secure platforms for sharing information, establishing clear procedures for classifying and depersonalising incident data and defining conditions and restrictions for using such information. It is advisable to consider the possibility of creating specialised judicial institutions or units that would deal with cases related to cybercrime and violations in the field of cybersecurity to strengthen the effectiveness of implementing laws in the field of preventing threats to critical infrastructure. This will allow for a more professional and efficient handling of such cases, considering their technical complexity and specifics.

International cooperation in the protection of critical infrastructure. As part of the globalisation of threats to the digital space and their cross-border nature, global cooperation in preventing threats to critical infrastructure is becoming of paramount importance for Ukraine. According to the Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), one of the key principles of ensuring the protection of the digital space is global interaction to strengthen mutual confidence in the field of digital security and develop coordinated strategies to combat network hazards. In this context, Ukraine's participation in international initiatives, such as the Convention on Cybercrime (2001), which creates a legislative framework for global interaction in countering cybercrime, is especially important.

An essential component of transnational cooperation is the coordination of national legislation of Ukraine with EU norms in the field of critical infrastructure protection (Chumachenko & Popel, 2023). In particular, the implementation of the Directive of the European Parliament and of the Council No. 2016/1148 (2016) provisions on measures for a high joint level of security of network and information systems on the territory of the NIS Directive Union is a vital task for Ukraine within the framework of the association agreement with the EU. This harmonisation will create a single legal and technical space for the exchange of information about cyber incidents and joint response to cyber threats. A special role in international cooperation is played by Ukraine's cooperation with NATO in the field of preventing threats to the digital space. According to the annual national programme under the auspices of the NATO-Ukraine Commission, Ukraine actively participates in NATO cyber defence exercises, such as the "Cyber Coalition" and "Locked Shields". This cooperation allows Ukrainian specialists to gain valuable experience and increase their readiness to counter complex cyber-attacks on critical infrastructure facilities. In addition, within the framework of the NATO Digital Space Security Trust Fund for Ukraine, projects are being implemented to modernise critical infrastructure security systems.

At the regional level, Ukraine's cooperation within the framework of the Trimorya initiative, which unites the countries of Central and Eastern Europe (Ukraine becomes a..., 2022), is important. The initiative is developing common approaches to protecting cross-border critical infrastructure, particularly in the energy and transport sectors. Such cooperation is particularly relevant in the context of the integration of the energy systems of Ukraine and the EU, which requires an increased level of cybersecurity to ensure the stability of energy supplies. An important element of cross-border cooperation is Ukraine's participation in global initiatives to secure the digital space, in particular, within the framework of the United Nations. Ukraine, as an active participant in these initiatives, has the opportunity not only to adopt best practices but also to influence the formation of a global cybersecurity policy.

Cooperation with the EU in the field of critical infrastructure security goes beyond just harmonising legislation. An important element is Ukraine's participation in EU platforms and projects, such as Horizon Europe (European Commission, 2021) and the Digital Europe Programme (European Commission, 2022). These programmes provide access to advanced technologies and methodologies for securing critical infrastructure and facilitate the exchange of experience between specialists from different countries. Priority should be given to the opportunities that participation in the European Cybersecurity Competence Centre opens up, which can become a key tool for improving the cyber resilience of Ukrainian critical infrastructure.

Regarding bilateral relations in the field of preventing threats to the digital space, Ukraine actively cooperates with leading countries of the world. In particular, the Memorandum of Understanding between Ukraine and the USA Regarding Collaboration on Ukrainian Energy System Resilience (2021) provides for the dissemination of data on cyber risks, joint exercises, and technical assistance in protecting critical infrastructure. Similar agreements have been signed with the United Kingdom, Canada, Japan, and Australia, which allows creating a multi-layered system of international support in countering cyber risks. Special attention should be paid to the issue of international legal regulation of state responsibility for cyber-attacks on critical infrastructure facilities. In this context, Ukraine supports initiatives to create and implement the norms of a balanced policy of countries in the digital environment, especially within the framework of the United Nations Group of Governmental Experts (2021) on International Information Security. The development of international legal mechanisms for attributing cyber-attacks and bringing violator states to justice is a crucial task for ensuring global prevention of threats to the digital space and ensuring the security of Ukraine's national interests in the context of hybrid aggression.

The results obtained can be used to develop effective strategies for protecting critical infrastructure in Ukraine and improving the state structure of digital protection in the context of ongoing conflict. The implementation of the proposed recommendations will substantially increase the level of security of information networks of critical infrastructure of Ukraine, which will contribute to strengthening national security and resilience of the state in the face of constantly evolving cyber threats.

Discussion

The results of the study indicate a number of important aspects that require detailed discussion. Firstly, the examination of intrusions on the critical infrastructure of Ukraine in 2014-2023 showed a substantial increase in the number and complexity of attacks after the start of a full-scale invasion of the aggressor in 2022. This is consistent with the conclusions of R. Osei-Kyei *et al.* (2023), who noted the increased vulnerability of critical infrastructure to cyber threats in crisis situations. The results also support the observations of R. Cantelmi *et al.* (2021) on the importance of adaptive approaches to protecting information networks in the face of dynamic threats. It is worth noting that the increase in the number of attacks on critical infrastructure was also accompanied by an increase in their technological complexity and target orientation. There is a tendency to use more sophisticated methods of social engineering and targeted attacks on specific critical objects, which requires the formation of innovative methods for identifying and countering such threats.

R. White (2019) examines cybersecurity vulnerabilities in industrial control systems, highlighting sophisticated cyber threats and their impact on state security. Analysing past incidents, R. White (2019) identifies attack patterns and advocates for proactive defence mechanisms. L. Andrew (2020) expands on R. White (2019) work, focusing on power grids and communication networks. L. Andrew (2020) demonstrates how cyberattacks on one component can trigger cascading failures, using empirical evidence from large-scale incidents to emphasise the need for integrated security policies. E.D. Knapp (2024) explores evolving cyber threats and defence strategies, emphasising artificial intelligence and machine learning in threat mitigation. Author argues that traditional security measures are insufficient against adaptive adversaries and highlights recent advancements in cybersecurity technologies and regulations. Aligning with the present study, E.D. Knapp (2024) underscores the necessity of robust cybersecurity measures for Ukraine's critical infrastructure. The interconnectedness of strategically important objects, as noted in the aforementioned works, resonates with the cascading effects observed in Ukraine, where a successful attack on one component often leads to widespread disruptions across multiple sectors. Consequently, the conclusions of the present study corroborate the imperative for a systemic approach to enhance Ukraine's cybersecurity measures through the establishment of advanced legal frameworks and enhanced security protocols.

The challenges associated with the sustainability of urban critical infrastructure and the security of network infrastructure have been examined by K. Pipyros (2019) and O. Ivanenko (2020). Their research highlights the heightened vulnerability of urban infrastructures to cyber threats due to their complexity and concentration of critical assets. The emphasis on the need for comprehensive security strategies that integrate technical, organisational and social dimensions corresponds with the findings of the present study, which identifies weak authentication protocols and outdated cybersecurity measures as key risk factors. In line with their recommendations, this study advocates for the implementation of adaptive protection strategies, incorporating artificial intelligence and advanced anomaly detection mechanisms, to effectively mitigate risks to Ukraine's urban critical infrastructure.

The protection of key state resources in the context of military conflicts and hybrid threats has been explored by C. Pursiainen (2021) and M. Haber (2022). Their studies illustrate the transformation of national security approaches in response to hybrid threats, which combine cyberattacks with physical sabotage and information warfare, a phenomenon which is directly relevant to the current study. The latter focuses on the cybersecurity challenges faced by Ukraine amid ongoing military conflict. The findings of these studies lend support to the argument that traditional security measures are inadequate in the face of hybrid threats, underscoring the necessity for a coordinated strategy that integrates military, cybersecurity, and intelligence capabilities. The present study contributes to this body of knowledge by proposing targeted measures, such as the establishment of sector-specific cybersecurity centres and regular cybersecurity exercises, with the aim of enhancing national resilience against evolving threats.

An analysis of existing systems of protection of communication structures of critical infrastructure of Ukraine has shown that the most effective are integrated approaches that combine technical, organisational, and legal measures. This confirms the findings of D. Rehak *et al.* (2019) on the need for a comprehensive strategy to assess the sustainability of critical infrastructure elements. The study showed that the most successful organisations are those that have implemented a multi-level security system that includes not only modern technical solutions but also regular training of personnel, clear incident response protocols, and an effective risk management system. It was particularly important to implement the principles of "security by design" in the development and modernisation of critical infrastructure management systems, which is consistent with the recommendations of T. Loveček *et al.* (2021) on the use of modelling and simulation to improve the protection of critical infrastructure.

An important nuance identified during the analysis is the need for international cooperation in the field of critical infrastructure protection. This is especially true in the context of cross-border threats that arise in the context of hybrid warfare (Lyndyuk *et al.*, 2023). The results complement the conclusions of L. Newlove-Eriksson *et al.* (2018) on the relationship between the commercialisation of important information infrastructure and national security, emphasising the need for a balance between economic efficiency and security. The analysis showed that countries that actively participate in international initiatives to protect the digital space show a higher level of readiness to counter complex cyber threats. Especially valuable was the exchange of information about new types of attacks and methods of detecting them, which allows for a quick adaptation of security systems to evolving threats. This confirms the importance of Ukraine's participation in such international initiatives, as noted in the study by A.B. Darıcılı and S. Celik (2022).

Comparing of results with the study by W. Liu and Z. Song (2020) on the sustainability of urban critical infrastructure networks showed that in the context of military conflict, the role of backup systems and the ability to quickly recover from attacks increases substantially. This highlights the need to develop special security strategies adapted to the conditions of active confrontation (Palko *et al.*, 2023). The study determined that critical infrastructure facilities that have developed and regularly updated business continuity and disaster recovery plans show substantially higher resistance to cyber-attacks. Especially effective was the creation

of distributed and duplicated control systems, which allows quickly restoring the functioning of critical objects even in the event of a successful attack on one of the components. These findings are comparable to the recommendations provided by H. Riggs *et al.* (2023) on strategies to mitigate the impact of cyber-attacks on critical infrastructure.

The analysis of the security system of information networks of critical infrastructure of Ukraine revealed both strengths (for example, the appropriate qualification of specialists in the protection of digital space) and weaknesses (in particular, outdated equipment at some critical infrastructure facilities). These results correlate with the conclusions of M. Kovaliv *et al.* (2021) on the need to improve legal support for the protection of the digital space of critical infrastructure in Ukraine. The analysis also showed that the strong point of the Ukrainian cyber defence system is the ability to quickly adapt to new threats and the high motivation of personnel. However, insufficient funding, especially in the regions, and the lack of a unified national strategy for cyber protection of critical infrastructure remain weak points. These factors pose substantial risks in the face of constantly evolving cyber threats.

Cyber-attacks on critical infrastructure information networks are a leading challenge to the country's state stability in the conflict with the aggressor (Yefimenko *et al.*, 2023a). This confirms the conclusions of I. Sopilko *et al.* (2022) on the substantial role of information wars in threats to Ukraine's information security. Experts also noted the growing role of artificial intelligence and machine learning both in the development of new attack methods and the creation of security systems. Special attention was paid to the need to develop a system for early detection of cyber threats and improve interagency coordination in responding to incidents. In addition, experts stressed the importance of increasing the electronic (digital) education of citizens as a key factor in countering cyber threats.

The main result is the need for continuous adaptation of security systems to new types of threats. This reflects the study by A. Djenna *et al.* (2021) which highlighted new challenges in protecting the digital space related to the development of the Internet of Things in the context of critical infrastructure. The study expands on these findings, indicating that in the context of active military conflict, the rate of emergence of new types of threats increases substantially, which requires the introduction of flexible and adaptive security systems. The importance of this statement lies in the fact that it highlights the need to move from static security models to dynamic ones that can quickly adapt to transformations in the threat landscape. This has important implications for the development of cybersecurity policies and strategies at the national level and planning investments in the development of critical infrastructure security systems.

The analysis showed the need to improve the legislative framework of Ukraine regarding threat prevention in critical infrastructure, especially in terms of defining responsibility and coordinating the actions of various departments. This complements the conclusions of M. Sokiran (2021) on the basic principles of public administration of critical infrastructure in Ukraine. However, the present study goes further, showing that in hybrid warfare, the existing regulatory framework is often not flexible enough to effectively respond to rapidly changing threats. This underscores the importance of developing new legislative mechanisms that would allow legal norms to be quickly adapted to new challenges without losing their effectiveness and legitimacy. This approach is consistent with the recommendations of C.M. Newbill (2019) on the need for a global approach to identifying and preventing threats to critical infrastructure.

Analysis of the report of the European Union Agency for Cybersecurity on the threat landscape for critical infrastructure of Ukraine determined common features and differences in approaches to cybersecurity between Ukraine and the EU countries (Cloud consciousness: Industry…, 2015). Thus, the growing role of state-sponsored cyber-attacks and the need to develop cross-border cooperation in the exchange of information on cyber threats are noted. These findings highlight the importance of Ukraine's further integration into the European cybersecurity system.

S.A. Mitoulis *et al.* (2023), reviewing the development of a framework for the sustainability of critical infrastructure in conflict situations showed that Ukraine faces unique challenges that require innovative approaches to ensuring cyber resilience. In particular, the authors established that traditional risk assessment methods are often ineffective in high-intensity conflict environments, where threats can change rapidly and combine in unpredictable ways. This highlights the importance of developing new risk assessment and security planning methodologies that consider the specifics of hybrid threats and rapidly changing security environments.

A key element of the study was the identification of the vital role of the human factor in ensuring the prevention of threats to the digital space of critical infrastructure. Although this is partially consistent with the statement of M.J. Khan (2023) on the importance of staff training, the study delves deeper, showing that in active conflict situations, the effectiveness of threat prevention often depends on the ability of staff to make quick and unconventional decisions under high stress. This points to the need to develop new approaches to training cybersecurity professionals that include not only technical skills, but also the development of critical thinking, stress tolerance, and the ability to adapt quickly.

Prospects for further research include the need for a more thorough study of the correlation between the physical safety and cybersecurity of critical infrastructure facilities in conflict situations. This aligns with the findings of E. Izycki and E.W. Vianna (2021) on critical infrastructure as a battlefield for cyber warfare, but the study highlights the need to develop integrated threat prevention approaches that consider both cybernetic and physical aspects of security. An important area of future research is also the development of methods for predicting and early detection of new types of cyber threats, which is exceptionally important in the context of the use of advanced technologies by the enemy, such as machine computing (artificial intelligence).

Scenario modelling of potential cyber-attacks has shown that the energy and financial sectors of critical infrastructure remain the most vulnerable. This is consistent with the paper of A. Abedi *et al.* (2019), which noted the high vulnerability of energy systems to cyber-attacks. However, contrary to their findings, the study showed that in the context of active military conflict, the vulnerability of transport and telecommunications infrastructure also increases substantially. Modelling various attack scenarios allowed identifying potential vulnerability points and assessing possible cascading effects in the event of a successful attack on one of the key objects. The results of this simulation highlight the need to develop comprehensive response plans for various types of

cyber-attacks, including scenarios of simultaneous attacks on various sectors of critical infrastructure. The results draw attention to the crucial importance of continuous improvement of threat prevention systems for information networks of critical infrastructure of Ukraine in the context of the ongoing conflict with Russia. They also indicate the expediency of continuing scientific research in this area, in particular, the development of innovative methods for detecting and countering new types of cyber-attacks.

Conclusions

The conducted study allowed obtaining a number of practical results. The analysis identified substantial discrepancies between the existing state of security in the state and international standards, especially in terms of technical support and investment. It was established that after the start of a full-scale Russian invasion on February 24, 2022, the number and complexity of cyber-attacks on strategically important objects in Ukraine has substantially increased, which emphasises the need to strengthen digital defence methods. The study confirmed the effectiveness of integrated protection approaches that combine technical, organisational, and legal measures. Organisations that have implemented a multi-level security system demonstrate higher resistance to cyber-attacks. Most experts consider cyber-attacks on critical infrastructure information networks to be one of the biggest threats to Ukraine's national security in a conflict situation.

A significant challenge confronting Ukraine is the alignment of its cybersecurity legislation with international norms, such as the EU's NIS 2 Directive and NATO protocols. There are evident deficiencies in the categorisation of critical infrastructure, compliance standards, and liability measures. Legal fragmentation and inadequate interagency coordination impede cybersecurity efforts, and the absence of a unified national cyber defence strategy exacerbates vulnerabilities. A comparative analysis reveals that leading cybersecurity frameworks in the USA, UK, and Germany enforce stricter compliance and oversight. In order to address these challenges, Ukraine must adopt advanced risk assessment strategies and establish a dedicated national cybersecurity agency with expanded authority to enforce standards and coordinate resilience efforts.

Furthermore, stronger legal frameworks for public-private partnerships are required. Unlike the USA's Critical Infrastructure Partnership Advisory Council, Ukraine lacks structured collaboration between state authorities and private operators. Incentives for private sector participation in cybersecurity investments and information-sharing should be expanded. International cooperation is vital for countering cyber threats. While Ukraine is a participant in the Convention on Cybercrime and NATO initiatives, additional legal provisions are required for cross-border data exchange, incident reporting, and coordinated cyber defence. The study recommends accelerating international cybersecurity standard adoption, strengthening legislative mechanisms, and enhancing accountability for cyber incidents. These measures will improve Ukraine's cyber resilience through regulatory consistency, institutional capacity-building, and more effective responses to emerging threats. Legal adaptation to global best practices is essential to mitigate evolving cybersecurity risks. During the analysis of the regulatory framework of Ukraine, certain gaps were identified in regulating the protection of critical infrastructure in a hybrid war. The existing regulatory framework is often not flexible enough to effectively respond to rapidly changing threats. This underlines the need to develop new legislative mechanisms that would provide for a quick adaptation of legal norms to meet new challenges without losing their effectiveness and legitimacy.

The study had certain limitations related to the partial availability of data on the real state of security of important infrastructure for national security reasons, as well as the rapidly changing situation in conditions of active conflict. For further research, it is recommended to focus on developing methods for predicting and early detecting new types of cyber threats and examining the relationship between the physical safety and cybersecurity of critical infrastructure facilities in conflict situations.

Acknowledgements

None.

Conflict of interest

None.

References

[1] Abedi, A., Gaudard, L., & Romerio, F. (2019). Review of major approaches to analyze vulnerability in power system. *Reliability Engineering & System Safety*, 183, 153-172. doi: 10.1016/j.ress.2018.11.019.

[2] Act on the Federal Office for Information Security (BSI Act – BSIG). (2009, August). Retrieved from https://surl.li/gmcaco.

[3] Anakhov, P., Zhebka, V., Popereshnyak, S., Skladannyi, P., & Sokolov, V. (2023). Protecting objects of critical information infrastructure from wartime cyber attacks by decentralizing the telecommunications network. *Cybersecurity Providing in Information and Telecommunication Systems*, 3550, 240-245.

[4] Andrew, L. (2020). The vulnerability of vital systems: How "critical infrastructure" became a security problem. In M.A. Dunn & K.S. Kristensen (Eds.), *Securing "The Homeland"* (pp. 17-39). London: Routledge. doi: 10.4324/9780203926529.

[5] Cali, Ü., Catak, F.Ö., Balogh, Z.G., Ugarelli, R., & Jaatun, M.G. (2023). Cyber-physical hardening of the digital water infrastructure. In *Proceedings of the 2023 European interdisciplinary cybersecurity conference (EICC '23)* (pp. 181-188). New York: Association for Computing Machinery. doi: 10.1145/3590777.3591408.

[6] Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, 41, 341-376. doi: 10.1007/s10669-020-09795-8.

[7] Chernysh, R., Chekhovska, M., Stoliarenko, O., Lisovska, O., & Lyseiuk, A. (2023). Ensuring information security of critical infrastructure objects as a component to guarantee Ukraine's national security. *Amazonia Investiga*, 12(67), 87-95. doi: 10.34069/AI/2023.67.07.8.

[8] Chumachenko, S., & Popel, V. (2023). A systematic approach to the automation of the processes of ensuring personnel competence at critical infrastructure facilities of the defense forces of Ukraine. *Bulletin of Cherkasy State Technological University*, 28(3), 141-155. doi: 10.24025/2306-4412.3.2023.288836.

[9] Cloud consciousness: Industry group speaks out. (2015). Retrieved from https://digital-strategy.ec.europa.eu/en/library/cloud-consciousness-industry-group-speaks-out
[10] Convention on Cybercrime. (2001, November). Retrieved from https://surl.gd/uxuxjl.
[11] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2341-14#Text.
[12] Critical Infrastructure Partnership Advisory Council. (2023). Retrieved from https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac.
[13] Cybersecurity and Infrastructure Security Agency Act. (2018, November). Retrieved from https://surl.gd/bfcepu.
[14] Darıcılı, A.B., & Celik, S. (2022). National security 2.0: The cyber security of critical infrastructure. *PERCEPTIONS: Journal of International Affairs*, 26(2), 259-276.
[15] Davydiuk, A., & Potii, O. (2024). *National cybersecurity governance: UKRAINE*. Retrieved from https://ccdcoe.org/library/publications/national-cybersecurity-governance-ukraine/.
[16] Davydiuk, A., & Zubok, V. (2023). Analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats in times of war. In *15th international conference on cyber conflict: Meeting reality* (pp. 121-139). Tallinn: Institute of Electrical and Electronics Engineers. doi: 10.23919/CyCon58705.2023.10181813.
[17] Decree of the President of Ukraine No. 242/2016 "On the National Coordination Centre for Cybersecurity". (2016, June). Retrieved from https://zakon.rada.gov.ua/laws/show/242/2016#Text.
[18] Decree of the President of Ukraine No. 392/2020 "On the Decision of the National Security and Defence Council of Ukraine of 14 September 2020 "On the National Security Strategy of Ukraine". (2020, September). Retrieved from https://www.president.gov.ua/documents/3922020-35037.
[19] 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, May). Retrieved from https://www.president.gov.ua/documents/4472021-40013.
[20] Directive of the European Parliament and of the Council No. 2016/1148 "Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union". (2016, July). Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj.
[21] Djenna, A., Harous, S., & Saidouni, D.E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, 11(10), article number 4580. doi: 10.3390/app11104580.
[22] European Commission. (2021). *Horizon Europe*. Retrieved from https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
[23] European Commission. (2022). *Digital Europe Programme*. Retrieved from https://surl.li/hycdxt.
[24] Fuster, G.G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European Union: The digital, the critical and fundamental rights. In M. Christen, B. Gordijn & M. Loi (Eds.), *The ethics of cybersecurity* (pp. 97-115). Cham: Springer. doi: 10.1007/978-3-030-29053-5_5.
[25] Haber, M. (2022). Great power competition: Critical infrastructure. In A. Farhadi, R.P. Sanders & A. Masys (Eds.), *The great power competition: Cyberspace: The fifth domain* (pp. 3-26). Cham: Springer. doi: 10.1007/978-3-031-04586-8_1.
[26] Ivanenko, O. (2020). Implementation of risk assessment for critical infrastructure protection with the use of risk matrix. *ScienceRise*, 2, 26-38. doi: 10.21303/2313-8416.2020.001340.
[27] Izycki, E., & Vianna, E.W. (2021). Critical infrastructure: A battlefield for cyber warfare? In *16th International conference on cyber warfare and security* (pp. 454-464). London: Academic Conferences Limited.
[28] Kelemen, R. (2023). The impact of the Russian-Ukrainian hybrid war on the European Union's cybersecurity policies and regulations. *Connections*, 22(2), 75-90. doi: 10.11610/Connections.22.2.55.
[29] Key consequences of Russian aggression for Ukraine's water resources for 19-25 May 2022. (2022). Retrieved from https://davr.gov.ua/news/klyuchovi-naslidki-rosijskoi-agresii-dlya-vodnih-resursiv-ukraini-za-1925-travnya-2022-roku.
[30] Khan, M.J. (2023). Securing network infrastructure with cyber security. *World Journal of Advanced Research and Reviews*, 17(2), 803-813. doi: 10.30574/wjarr.2023.17.2.0308.
[31] Knapp, E.D. (2024). *Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems*. London: Syngress. doi: 10.1016/C2022-0-02315-1.
[32] Kovaliv, M., Skrynkovskyy, R., Nazar, Y., Yesimov, S., Krasnytskyi, I., Kaydrovych, K., Kniaz, S., & Kemska, Y. (2021). Legal support of cybersecurity of critical information infrastructure of Ukraine. *Path of Science*, 7(4), 2011-2018. doi: 10.22178/pos.69-12.
[33] Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2023, November). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20.
[34] Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2163-19#Text.
[35] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://www.president.gov.ua/documents/2297vi-11567.
[36] Law of Ukraine No. 2824-IV "On Ratification of the Convention on Cybercrime". (2005, September). Retrieved from https://zakon.rada.gov.ua/laws/show/2824-15#Text.
[37] Liu, W., & Song, Z. (2020). Review of studies on the resilience of urban critical infrastructure networks. *Reliability Engineering & System Safety*, 193, article number 106617. doi: 10.1016/j.ress.2019.106617.
[38] Loveček, T., Straková, L., & Kampová, K. (2021). Modeling and simulation as tools to increase the protection of critical infrastructure and the sustainability of the provision of essential needs of citizens. *Sustainability*, 13(11), article number 5898. doi: 10.3390/su13115898.

[39] Lyndyuk, A., Boiko, V., Bruh, O., Olishchuk, P., & Rurak, I. (2023). Development of international cooperation of the borderline territorial communities of Ukraine with the EU countries under martial law. *Financial and Credit Activity: Problems of Theory and Practice*, 5(52), 244-255. doi: 10.55643/fcaptp.5.52.2023.4161.

[40] Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law & Security Review*, 41, article number 105502. doi: 10.1016/j.clsr.2020.105502

[41] Memorandum of Understanding between Ukraine and the USA Regarding Collaboration on Ukrainian Energy System Resilience. (2021, September). Retrieved from https://ua.usembassy.gov/memorandum-of-understanding-between-ukraine-and-the-usa-regarding-collaboration-on-ukrainian-energy-system-resilience/.

[42] Mitoulis, S.A., Argyroudis, S., Panteli, M., Fuggini, C., Valkaniotis, S., Hynes, W., & Linkov, I. (2023). Conflict-resilience framework for critical infrastructure peacebuilding. *Sustainable Cities and Society*, 91, article number 104405. doi: 10.1016/j.scs.2023.104405.

[43] Network and Information Systems Regulations. (2018, April). Retrieved from https://www.legislation.gov.uk/uksi/2018/506/contents/made.

[44] Newbill, C.M. (2019). Defining critical infrastructure for a global application. *Indiana Journal of Global Legal Studies*, 26(2), 761-779.

[45] Newlove-Eriksson, L., Giacomello, G., & Eriksson, J. (2018). The invisible hand? Critical information infrastructures, commercialisation and national security. *International Spectator*, 53(2), 124-140. doi: 10.1080/03932729.2018.1458445.

[46] NIS 2 Directive. (2024). Retrieved from https://www.nis-2-directive.com/.

[47] Osei-Kyei, R., Almeida, L.M., Ampratwum, G., & Tam, V. (2023). Systematic review of critical infrastructure resilience indicators. *Construction Innovation*, 23(5), 1210-1231. doi: 10.1108/CI-03-2021-0047.

[48] Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber security risk modeling in distributed information systems. *Applied Sciences (Switzerland)*, 13(4), article number 2393. doi: 10.3390/app13042393.

[49] Pipyros, K. (2019). *A new systematic modelling methodology for improving cyber-attack evaluation on states Critical Information Infrastructure (CII)*. Athens: Athens University Economics and Business.

[50] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, June). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and.

[51] Pursiainen, C. (2021). Russia's critical infrastructure policy: What do we know about it? *European Journal for Security Research*, 6, 21-38. doi: 10.1007/s41125-020-00070-0.

[52] Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, 25, 125-138. doi: 10.1016/j.ijcip.2019.03.003.

[53] Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p "On Approval of the General Requirements for Cyber Defence of Critical Infrastructure Objects". (2019, June). Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

[54] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M.A., Amir, A., Vuda, K.V., & Sarwat, A.I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, 23(8), article number 4060. doi: 10.3390/s23084060.

[55] Schmitt, M.N. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Retrieved from https://lawcat.berkeley.edu/record/199769.

[56] Semenchenko, A., Pleskach, V., Zaiarnyib, O., & Pleskachb, M. (2020). Cyber security and cyber protection: The current state of public administration in Ukraine. In I. Sergienko & P. Andon (Eds.), *Proceedings of the 12th international scientific and practical conference of programming (UkrPROG 2020)* (pp. 276-284). Kyiv: CEUR Workshop Proceedings.

[57] Shahini, E., Fedorchuk, M., Hruban, V., Fedorchuk, V., & Sadovoy, O. (2024). Renewable energy opportunities in Ukraine in the context of blackouts. *International Journal of Environmental Studies*, 81(1), 125-133. doi: 10.1080/00207233.2024.2320021.

[58] Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: Legal and organizational support in leading countries, NATO and EU standards. *Journal of Security and Sustainability Issues*, 9(3), 977-992.

[59] Sokiran, M. (2021). Basic principles of public administration of critical information infrastructure: The example of Ukraine. *Advanced Space Law*, 7, 63-72.

[60] Sopilko, I., Svintsytskyi, A., Krasovska, Y., Padalka, A., & Lyseiuk, A. (2022). Information wars as a threat to the information security of Ukraine. *Conflict Resolution Quarterly*, 39(3), 333-347. doi: 10.1002/crq.21331.

[61] The history of the NotPetya virus: Should we be wary of similar cyberattacks in the future? (2018). Retrieved from https://www.imena.ua/blog/notpetya-cyberattack/.

[62] Ukraine becomes a partner in the Three Seas Initiative. (2022). Retrieved from https://www.eurointegration.com.ua/news/2022/06/21/7141676/.

[63] United Nations Charter. (1945, June). Retrieved from https://www.un.org/en/about-us/un-charter/full-text.

[64] United Nations. (2021). *Group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security*. Retrieved from https://www.un.org/disarmament/group-of-governmental-experts/.

[65] White, R. (2019). Risk analysis for critical infrastructure protection. In D. Gritzalis, M. Theocharidou & G. Stergiopoulos (Eds.), *Critical infrastructure security and resilience: Theories, methods, tools and technologies* (pp. 35-54). Cham: Springer. doi: 10.1007/978-3-030-00024-0_3.

[66] Yefimenko, I., Sakovskyi, A., & Bilozorov, Ye. (2023a). Protection of critical infrastructure as a component of Ukraine's national security. *Law Journal of the National Academy of Internal Affairs*, 13(2), 74-85. doi: 10.56215/naia-chasopis/2.2023.74.

[67] Yefimenko, I., Slipchenko, V., & Vaško, A. (2023b). Critical infrastructure as an object of criminal encroachment: General characteristics and features of the investigation organisation. *Scientific Journal of the National Academy of Internal Affairs*, 28(2), 41-51. doi: 10.56215/naia-herald/2.2023.41.

[68] Zhang, H., Huang, C., & Lyu, A. (2024). A compliance-enhancing approach to separated continuous auditing of intelligent endpoints security in war potential network based on location-sensitive hashing. In Y. Zhang, L. Qi, Q. Liu, G. Yin & X. Liu (Eds.), *Proceedings of the 13th international conference on computer engineering and networks* (pp. 100-119). Singapore: Springer. doi: 10.1007/978-981-99-9247-8 11.

Шляхи вдосконалення правового регулювання захисту інформаційних мереж критичної інфраструктури

Олександр Головко

Кандидат наук з державного управління
Національна академія Служби безпеки України
03066, вул. Михайла Максимовича, 22, м. Київ, Україна
https://orcid.org/0009-0004-9576-7737

Олена Кравченко

Кандидат юридичних наук, завідувач наукової лабораторії
Національна академія Служби безпеки України
03066, вул. Михайла Максимовича, 22, м. Київ, Україна
https://orcid.org/0000-0003-0246-1022

Микола Погребицький

Доктор юридичних наук, професор
Національна академія Служби безпеки України
03066, вул. Михайла Максимовича, 22, м. Київ, Україна
https://orcid.org/0000-0003-0779-6577

Іван Романюк

Кандидат юридичних наук
Національна академія Служби безпеки України
03066, вул. Михайла Максимовича, 22, м. Київ, Україна
https://orcid.org/0000-0003-4788-8046

Анотація. Дослідження було спрямоване на визначення шляхів удосконалення правового регулювання захисту інформаційних мереж критичної інфраструктури України, враховуючи сучасні виклики у сфері кібербезпеки та міжнародні стандарти. У роботі використано порівняльний аналіз законодавства України, ЄС, США та Великої Британії, що регулює кібербезпеку критичної інфраструктури, а також проведено оцінку ефективності чинних нормативно-правових актів у контексті сучасних загроз, зокрема збройного конфлікту. Аналіз виявив фрагментарність чинного законодавства, відсутність ефективного механізму координації державних органів, а також недостатність правових інструментів для регулювання відповідальності за кіберзлочини, спрямовані на критичну інфраструктуру. Встановлено, що нормативна база України лише частково відповідає міжнародним стандартам, що ускладнює її гармонізацію з вимогами ЄС. Недостатня інтеграція державного та приватного секторів у сфері кібербезпеки також є суттєвим чинником, що стримує ефективність захисту стратегічних цифрових об'єктів. Для підвищення ефективності правового регулювання необхідно здійснити комплексну гармонізацію законодавства України з нормами ЄС, зокрема з Директивою NIS 2, що визначає єдині вимоги до захисту критичної інфраструктури. Доцільним є запровадження обов'язкової сертифікації кібербезпекових заходів, а також розширення кримінальної відповідальності за кібератаки на критичну інфраструктуру, включаючи санкції для юридичних осіб. Важливим напрямом є законодавче закріплення створення єдиної національної системи моніторингу кіберзагроз і вдосконалення механізмів державно-приватного партнерства. Запропоновані зміни сприятимуть підвищенню рівня кіберстійкості критичної інфраструктури України, її відповідності міжнародним стандартам та інтеграції у глобальну систему кібербезпеки

Ключові слова: кіберстійкість; цифровий простір; стратегічні об'єкти; кіберзагрози; національна безпека