DOI: 10.52363/passa-2026.1-26
UDC: 351.862:620.9

Shchepanskiy E., *Doctor of Science in Public Administration, Professor, Head of the Department of Public Management and Administration, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi,*
ORCID: 0000-0001-7404-3722

Kopanchuk V., *Doctor of Science in Public Administration, Associate Professor, Professor of the Department of Public Management and Administration, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi*
ORCID: 0000-0002-4198-6510

Kravchuk O., *Doctor of Science in Public Administration, Professor, Professor of the Department of Criminal Law and Procedure, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi*
ORCID: 0000-0002-7002-4070

Щепанський Е., *доктор наук з державного управління, професор, завідувач кафедри публічного управління та адміністрування, Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький*

Копанчук В., *доктор наук з державного управління, доцент, професор кафедри публічного управління та адміністрування, Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький*

Кравчук О., *доктор наук з державного управління, професор, професор кафедри кримінального права та процесу, Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький*

SECURITY AND PROTECTION OF CRITICAL ENERGY INFRASTRUCTURE IN THE SYSTEM OF NATIONAL SECURITY OF THE STATE

БЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

The article examines the theoretical and applied aspects of ensuring the security of critical energy infrastructure within the system of national security of the state. It is substantiated that critical energy infrastructure is a key component of national security, as it ensures the functioning of the economy, the stability of public administration, and the continuity of social processes. Disruptions in its operation may lead to significant economic and social consequences that negatively affect the resilience of the state. The regulatory and legal framework for the protection of critical infrastructure in Ukraine is analyzed, in particular the Law of Ukraine "On Critical Infrastructure" and the National Security Strategy. It is established that effective protection requires a comprehensive combination of legal, organizational, technical, and informational measures aimed at preventing threats and minimizing their consequences. The main threats to the functioning of energy infrastructure are identified, including military attacks, cyber threats, man-made accidents, deterioration of networks, and insufficient modernization. These threats have become especially relevant under conditions of full-scale war, when energy facilities have become priority targets of attacks. The international experience of EU and NATO countries in enhancing the resilience of energy systems is analyzed. It is determined that key elements include the development of risk management systems, the implementation of digital technologies, strengthening cybersecurity, and international cooperation. It is substantiated that for Ukraine, priority areas include modernization of energy networks, development of backup energy supply systems, implementation of advanced cybersecurity technologies, improvement of public policy in this field, and strengthening coordination among security stakeholders.

e-ISSN 2786-5533

Keywords: *critical infrastructure, energy infrastructure, national security, energy security, cybersecurity, protection of critical facilities, public administration, resilience of energy systems.*

У статті досліджено теоретичні та прикладні аспекти забезпечення безпеки критичної енергетичної інфраструктури в системі національної безпеки держави. Обґрунтовано, що вона є ключовою складовою національної безпеки, оскільки забезпечує функціонування економіки, стабільність державного управління та безперервність соціальних процесів. Порушення її роботи може спричинити значні економічні й соціальні наслідки, що негативно впливають на стійкість держави. Проаналізовано нормативно-правові засади захисту критичної інфраструктури в Україні, зокрема Закон України «Про критичну інфраструктуру» та Стратегію національної безпеки. Встановлено, що ефективний захист потребує поєднання правових, організаційних, технічних та інформаційних заходів, спрямованих на запобігання загрозам і мінімізацію їх наслідків. Визначено основні загрози функціонуванню енергетичної інфраструктури: військові атаки, кіберзагрози, техногенні аварії, зношеність мереж і недостатній рівень модернізації. Особливої актуальності ці загрози набули в умовах повномасштабної війни, коли енергетичні об'єкти стали пріоритетними цілями атак. Проаналізовано міжнародний досвід країн ЄС і НАТО щодо підвищення стійкості енергетичних систем. Встановлено, що ключовими елементами є розвиток ризик-менеджменту, впровадження цифрових технологій, посилення кіберзахисту та міжнародна співпраця. Обґрунтовано, що для України пріоритетними є модернізація енергетичних мереж, розвиток резервного енергопостачання, впровадження сучасних технологій кіберзахисту та вдосконалення державної політики у цій сфері, а також підвищення рівня координації між суб'єктами забезпечення безпеки.

Ключові слова: *критична інфраструктура, енергетична інфраструктура, національна безпека, енергетична безпека, державна політика, кібербезпека, захист критичних об'єктів, енергетична система.*

Problem Statement. In the context of global instability, escalating geopolitical tensions, and rapid technological advancement, ensuring the security of critical infrastructure has emerged as a strategic priority for the functioning of the state. A pivotal role within this system is played by energy infrastructure, the stability of which underpins the continuity of economic processes, the functioning of public authorities, and the operation of essential societal systems.

Energy infrastructure ensures the generation, transmission, distribution, and supply of energy resources, thereby playing a crucial role in maintaining the economic resilience of the state and an adequate standard of living for the population. For this reason, the protection of energy facilities constitutes a key area of public policy within the national security system.

The relevance of this research has significantly increased in the context of the full-scale war, during which Ukraine's energy infrastructure has become one of the primary targets of missile and drone attacks. The destruction of power plants, substations, and energy networks creates substantial risks for the stable functioning of both the economy and the social sphere, while also increasing the likelihood of large-scale crisis situations. These challenges necessitate the development of a comprehensive system for protecting energy facilities that integrates legal, organizational, technical, and information security mechanisms.

Strategic documents play a pivotal role in shaping state policy in the field of critical energy infrastructure protection, as they define priorities and directions for ensuring national security. These include the National Security Strategy of Ukraine "Human Security – Country Security" [1], the Energy Security Strategy of Ukraine [2], and the Cybersecurity Strategy of Ukraine "Secure Cyberspace as a Key to the Country's Successful Development" [3], along with other policy documents aimed at enhancing the resilience of critical infrastructure. These documents establish a set of measures for preventing threats, responding to crisis situations, and restoring the functioning of energy systems, while also providing for the integration of international standards and best practices into the national security system.

e-ISSN 2786-5533

In addition to military threats, key risk factors affecting energy infrastructure include cyber threats, industrial accidents, the deterioration of energy networks, and the insufficient level of modernization of energy systems. In the context of the digitalization of the energy sector, cybersecurity is of particular importance, as cyberattacks can disrupt the functioning of energy systems and lead to large-scale interruptions in energy supply.

International experience demonstrates that the effective protection of critical energy infrastructure requires the implementation of risk management systems, the development of interagency coordination mechanisms, and active international cooperation in the field of energy security. Countries of the European Union and NATO place significant emphasis on enhancing the resilience of energy systems to crisis situations, which involves the modernization of energy networks, the development of backup energy sources, and the strengthening of cybersecurity for energy facilities.

Thus, ensuring the security and protection of critical energy infrastructure represents a key priority of state policy in the field of national security and should be implemented in accordance with national strategic frameworks. The development of an effective system for managing the security of energy infrastructure should be based on a comprehensive approach that includes improving the regulatory framework, implementing strategic priorities, introducing advanced technologies for protecting energy systems, and adapting international experience to the specific conditions of Ukraine's development.

Analysis of recent research and publications. The issues of ensuring the security of critical infrastructure and enhancing the resilience of energy systems have become the subject of extensive scholarly inquiry across the fields of public administration, national security, economics, and energy policy. The growing number of global challenges associated with military conflicts, industrial risks, and cyber threats has intensified academic attention to the protection of critical infrastructure, particularly within the energy sector.

The theoretical and methodological foundations of national security and its components are reflected in the works of Ukrainian scholars. In particular, H. P. Sytnyk has made a significant contribution by conceptualizing national

security as a comprehensive system aimed at protecting the vital interests of the state, society, and individuals from internal and external threats. Within this framework, an effective national security system is understood to rely on the interaction of political, economic, social, and energy-related mechanisms that ensure state stability [4].

Issues related to energy security and its role in strengthening national resilience are also addressed in studies conducted by experts of the Razumkov Centre. These works emphasize that energy infrastructure constitutes a key component of the state's strategic security system, as its functioning directly affects economic stability, defense capability, and social cohesion. The war initiated by the Russian Federation against Ukraine is characterized by deliberate attacks on energy infrastructure facilities aimed at weakening the country's economic potential [5].

Important aspects of warfare in its military, political, economic, social, humanitarian, and informational dimensions, as well as its impact on economic and energy security, are examined in the works of V. P. Horbulin [6], Ya. A. Zhalilo [7], and V. V. Ksendzuk [8]. These studies consider the energy sector as one of the key domains for ensuring economic resilience and emphasize the need to develop effective public policy mechanisms for the protection of critical infrastructure.

The issue of protecting critical infrastructure is also extensively addressed in international analytical research. Reports by the International Energy Agency (IEA) highlight that energy systems are among the most vulnerable elements of modern infrastructure due to their integration of complex technological networks, digital control systems, and international energy markets. Disruptions in the functioning of energy systems can lead to large-scale economic losses and social crises [9; 10]. Reports by the Organization for Economic Co-operation and Development (OECD) emphasize that enhancing the resilience of critical infrastructure is a key priority of contemporary public policy. The main directions for ensuring its security include the development of risk management systems, improved coordination among public authorities, and the implementation of advanced digital technologies for monitoring and protecting infrastructure systems [11].

e-ISSN 2786-5533

A significant role in shaping international standards for the security of energy infrastructure is also played by studies and analytical materials of the European Union and NATO. Documents of the European Union Agency for Cybersecurity (ENISA) highlight the need to strengthen cybersecurity in energy systems, as the digitalization of energy infrastructure creates new vulnerabilities and potential threats [12]. At the same time, NATO materials place particular emphasis on enhancing the resilience of energy systems to hybrid threats, including military attacks, sabotage, and cyber operations [13; 14].

Thus, the analysis of scientific literature and international analytical research indicates a growing focus on the issue of ensuring the security of critical energy infrastructure. At the same time, a significant portion of existing studies tends to concentrate on specific aspects of energy or economic security, whereas the issue of comprehensive security management of energy infrastructure within the national security system requires further in-depth scholarly exploration.

Research objectives. The aim of the article is to examine the theoretical and applied aspects of ensuring the security and protection of critical energy infrastructure within the national security system, as well as to identify key directions for improving public policy aimed at enhancing the resilience of energy systems to contemporary threats and risks.

To achieve this aim, the study pursues the following objectives:

1. To clarify the concept of "critical infrastructure" and determine the role of energy infrastructure within the national security system.

2. To analyze the main threats to the functioning of critical energy infrastructure, including military, technogenic, and cyber threats affecting the stability of energy systems.

3. To examine international experience in ensuring the security of critical infrastructure, particularly the approaches of the European Union and NATO to enhancing energy system resilience.

4. To outline current challenges and key issues related to ensuring the security of critical energy infrastructure in Ukraine.

e-ISSN 2786-5533

5. To develop recommendations for improving public policy in the field of critical energy infrastructure protection, aimed at strengthening energy security and national resilience.

Presentation of the main material. The functioning of a modern state largely depends on the stability and continuity of critical infrastructure. According to Article 1 of the Law of Ukraine "On Critical Infrastructure," it is defined as a set of critical infrastructure objects, while, in accordance with paragraph 13 of part 1 of this Article, critical infrastructure objects are understood as facilities, systems, and their components whose disruption may lead to adverse consequences for national security, the economy, and public safety [15]. Such objects include, in particular, energy systems, transport networks, information and communication infrastructure, water supply systems, healthcare systems, and other strategically important sectors.

A central position within the structure of critical infrastructure is occupied by energy infrastructure, which ensures the generation, transmission, and distribution of energy resources. Its stable functioning constitutes a prerequisite for the uninterrupted operation of industry, transport, communications, healthcare institutions, and other spheres of public life, thereby determining its pivotal role in maintaining economic stability and national security.

Within the energy sector, critical infrastructure includes power plants, substations, high-voltage transmission networks, gas transmission systems, oil pipelines, and other strategically important energy facilities whose disruption may result in significant adverse consequences for the economy and public welfare.

Energy infrastructure is characterized by a complex structure comprising several interrelated subsystems:

– energy generation (power plants of various types);

– energy transmission (high-voltage networks and pipelines);

– energy distribution (local grids and supply systems);

– control and dispatching systems.

Disruption of any of these components may lead to substantial negative consequences for the national energy system. At the same time, in accordance

e-ISSN 2786-5533

with Article 3 of the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine," critical infrastructure facilities and their information systems are classified as cybersecurity objects. Furthermore, pursuant to Articles 6 and 8 of this Law, their protection involves the prevention of cyber threats and the enhancement of resilience to such threats, which is particularly relevant in the context of the ongoing digitalization of the energy sector [16].

The issue of energy infrastructure security has gained particular urgency in the context of the full-scale war in Ukraine. As noted by V. V. Ksendzuk and M. Yu. Pokotylo, the Russian-Ukrainian war has generated significant challenges for energy security, associated with the destruction of energy facilities, disruptions in the functioning of energy systems, and substantial economic losses, thereby necessitating a transformation of approaches to ensuring the stability of the energy sector [8].

In this context, the analysis of key threats affecting the functioning of critical energy infrastructure becomes especially important. The generalization of scientific research and international experience makes it possible to identify several major groups of threats that impact the stability of energy systems.

Table 1. Key Threats to Critical Energy Infrastructure

Threat Type	Description	Potential Consequences
Military threats	Missile and drone attacks, sabotage, and damage to energy facilities	Destruction of power plants, disruptions in energy supply
Cyber threats	Cyberattacks targeting energy network control systems	Disruption of energy system operations, power outages
Industrial accidents	Failures at power plants or energy networks	Disruptions in energy system functioning, significant economic losses
Infrastructure deterioration	Aging equipment and insufficient modernization	Increased failure rates and reduced reliability of energy networks

Source: compiled by the author based on [8; 17; 18; 19].

The conducted analysis indicates that critical energy infrastructure is exposed to a complex set of interrelated risks. Under current conditions, the most disruptive factors include military threats, cyber incidents, and their

associated secondary industrial effects, which may cause disruptions in energy supply, damage to key generation and transmission facilities, and destabilization of socio-economic processes within the state. At the same time, infrastructure deterioration and natural factors further exacerbate the overall vulnerability of energy systems and complicate their recovery.

Ensuring the security of critical energy infrastructure constitutes one of the priority areas of public policy in most developed countries. As evidenced by analytical studies, including the Green Paper on Critical Infrastructure Protection in Ukraine, an effective protection system should be based on the integration of legal, organizational, and technical mechanisms, a clear allocation of responsibilities among public authorities, critical infrastructure operators, and response entities, as well as the application of a risk-oriented management approach [11; 17].

An important dimension of ensuring the security of energy infrastructure is the strengthening of cybersecurity. In the context of the ongoing digitalization of the energy sector, a significant share of energy system management processes is carried out through information and communication technologies. While this enhances operational efficiency, it simultaneously increases vulnerability to cyber threats. As noted in scholarly research, cyberattacks may target dispatch control systems, automated control systems, and other elements of digital infrastructure, potentially leading to disruptions in energy supply and substantial economic losses [18]. In response, European Union countries place considerable emphasis on the implementation of advanced cybersecurity technologies, the establishment of cyber incident response centers, and the development of monitoring systems for cyber threats in the energy sector [12].

International analytical studies indicate that the functioning of modern energy systems is accompanied by a wide range of risks capable of undermining their reliability and resilience. These include military attacks, cyber threats, industrial accidents, infrastructure deterioration, and natural and climatic factors. The generalized distribution of these risks within the overall structure of threats to energy systems is presented in Figure 1. The distribution shown in Figure 1 is of an analytical and expert nature and has been developed

by the author through the systematization of international analytical materials on the key vulnerabilities of energy systems.

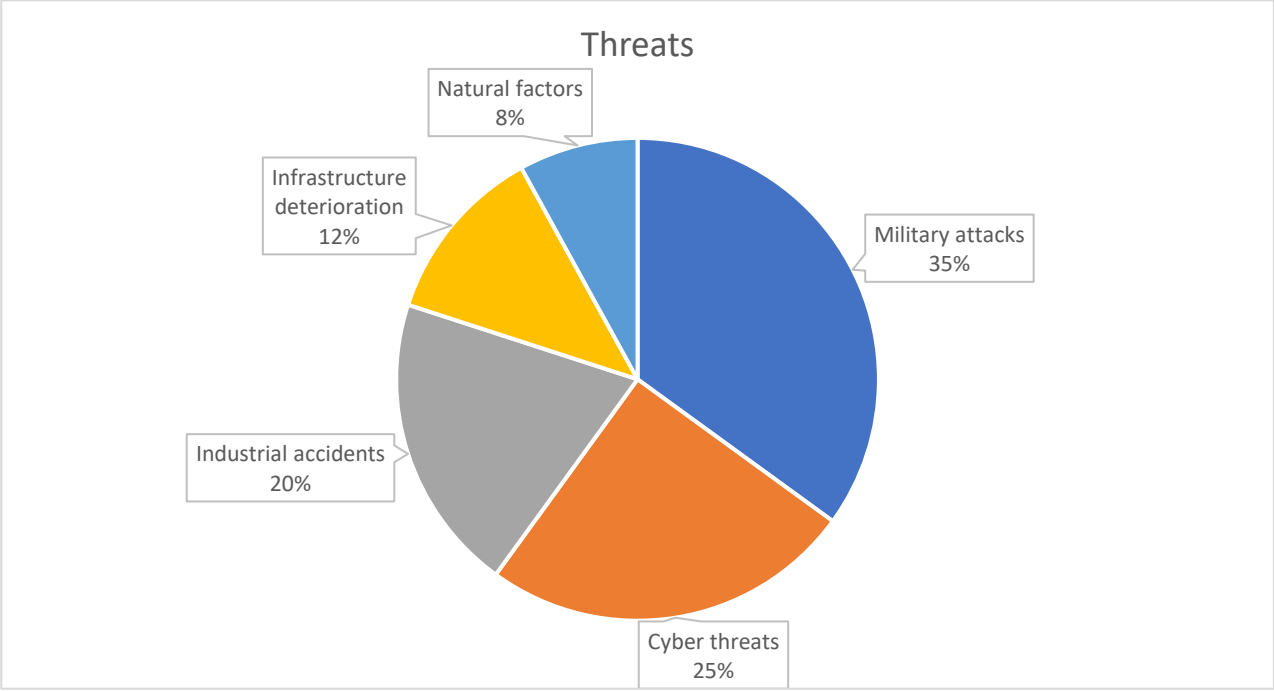

Figure 1. Analytical and Expert-Based Structure of Key Threats to Critical Energy Infrastructure in the International Context

Source: compiled by the author based on the systematization of [9; 10].

The conducted synthesis indicates that the largest share in the structure of threats to energy infrastructure is accounted for by military attacks and cyber threats. This can be explained by the fact that modern energy systems combine complex physical infrastructure with digital control systems, making them potential targets for both physical attacks and cyber operations. In contemporary security crises, energy infrastructure is often used as an instrument of pressure on the state, as its disruption may lead to significant economic losses and social instability.

At the same time, a considerable share of risks is associated with industrial accidents and infrastructure deterioration. In many countries, energy networks were built several decades ago, which necessitates their modernization and the introduction of advanced technologies for managing energy systems. For this reason, one of the key priorities of public policy in the field of energy security is the modernization of energy infrastructure, the

development of backup energy supply systems, and the enhancement of resilience of energy networks to crisis situations.

Thus, the analysis of international experience demonstrates that the effective protection of critical energy infrastructure is possible only through a comprehensive approach, which includes the development of risk management systems, modernization of energy networks, strengthening of cybersecurity, and active international cooperation in the field of energy security.

In view of the above, and taking into account the conditions of the full-scale war, the elevated level of military and cyber threats, as well as the deterioration of energy infrastructure, it is appropriate to generalize the structure of key threats to critical energy infrastructure in Ukraine, as presented in Figure 2. The distribution of threats shown in Figure 2 is also of an analytical and expert-based nature and reflects the author's synthesis of official international and national sources regarding the vulnerabilities of Ukraine's energy sector.

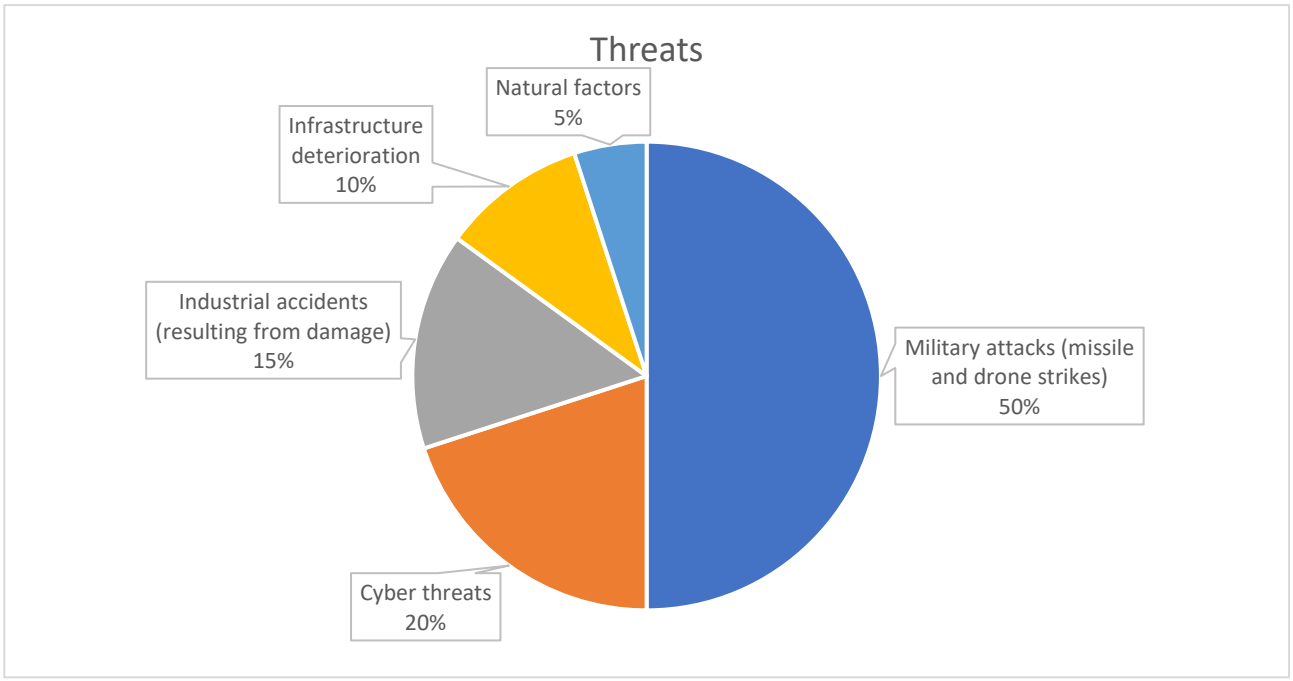

Figure 2. Analytical and Expert-Based Structure of Key Threats to Critical Energy Infrastructure in Ukraine under Current Conditions

Source: compiled by the author based on the systematization of [20–23].

The conducted synthesis provides grounds to assert that the structure of threats to Ukraine's critical energy infrastructure is dominated by military factors, which significantly distinguishes the national situation from global trends. This specificity is determined by the conditions of a full-scale war, in which energy facilities systematically serve as priority targets of missile and drone strikes, resulting in extensive destruction and disruption of the energy system's functioning.

The second most significant group of threats is represented by cyber threats, the relevance of which is driven by the high level of digitalization of the energy sector and the integration of information and communication technologies into management processes. The increasing intensity of cyberattacks during 2022–2026 indicates a growing vulnerability of critical infrastructure to cyber incidents, a substantial share of which is specifically targeted at energy facilities.

Industrial accidents also occupy an important place in the overall risk structure. Under current conditions, they often have a secondary nature, arising as a consequence of physical damage to energy infrastructure. The loss of generating capacity and the disruption of energy network integrity complicate the provision of stable energy supply and increase the likelihood of systemic failures.

Another significant risk factor is infrastructure deterioration, caused by the prolonged operation of a considerable share of energy networks and the insufficient level of their modernization. This reduces the reliability of energy system functioning and increases its vulnerability to both external and internal threats. Natural factors account for the smallest share in the overall risk structure; however, their impact may be significantly amplified under conditions of damaged or weakened infrastructure, thereby complicating recovery processes and the operation of energy facilities.

Thus, the structure of threats to Ukraine's critical energy infrastructure is characterized by a pronounced military dominance, which defines its specificity and distinguishes it from global patterns, where industrial and cyber risks tend to play a more prominent role. In this regard, the resilience of critical energy infrastructure should be considered not only as the ability to withstand threats,

but also as the capacity to ensure continuity of operation, localize the consequences of damage, and restore functionality within acceptable timeframes.

Ensuring such resilience requires the development of a coherent and scientifically grounded public policy aimed at strengthening the capacity of energy systems to withstand a wide range of threats. For Ukraine, this issue acquires a systemic character in the context of a full-scale war, which not only increases the intensity of external impacts but also necessitates a transformation of approaches to ensuring energy security. In this context, the protection of energy infrastructure becomes one of the key directions of state policy aimed at preserving the functional capacity of the economy and maintaining social stability.

The effectiveness of public policy in the field of critical energy infrastructure protection is determined by the ability to integrate legal, organizational, and technological instruments into a unified security management system. Such a system should be based on a risk-oriented approach that involves the identification, assessment, and prioritization of threats, the development of mechanisms for their prevention and mitigation, as well as a clear allocation of responsibilities among public authorities, critical infrastructure operators, and response entities. Equally important is ensuring the adaptability of governance decisions, which enables timely responses to evolving threats and supports an adequate level of resilience of energy systems.

In this context, the use of international experience becomes particularly important, as it demonstrates that enhancing the protection of critical infrastructure is achieved through the application of a systemic approach. Such an approach involves institutional coordination among public authorities, private sector actors, and international partners, ensuring consistency in responding to threats. In addition, international practice emphasizes the integration of advanced digital technologies into security management processes, which, while increasing operational efficiency, also contributes to heightened vulnerability to cyber threats [11; 12].

Taking this into account, strengthening the cybersecurity of energy infrastructure is one of the priority directions of public policy. This involves not

only the implementation of technical protection measures, but also the development of a comprehensive cybersecurity system, including cyber incident monitoring, institutional capacity building, and the improvement of personnel training. Such an approach ensures the continuity of energy system functioning under increasing cyber risks and minimizes the potential negative consequences of cyberattacks.

At the same time, structural modernization of energy infrastructure represents another key policy direction, as it constitutes a necessary prerequisite for improving its reliability and resilience. This includes upgrading outdated material and technical assets, implementing intelligent energy management systems, and developing backup and decentralized energy supply sources. The implementation of these measures contributes to the formation of a more flexible and resilient energy system capable of functioning effectively even under crisis conditions and partial damage to its components.

Therefore, ensuring the security of critical energy infrastructure requires a comprehensive integration of strategic, institutional, and technological solutions within the broader national security system. Such a multi-level model not only enables an effective response to existing threats but also creates the foundation for the long-term resilience of the energy sector under contemporary challenges. Taking into account international experience, the main directions for improving public policy in the field of critical energy infrastructure protection can be identified, as presented in Table 2.

Table 2. Main Directions for Improving Public Policy on the Protection of Critical Energy Infrastructure

Public Policy Direction	Key Content	Expected Outcome
Modernization of energy infrastructure	Upgrading energy networks and equipment	Increased reliability of the energy system
Strengthening cybersecurity	Implementation of cybersecurity systems for energy networks	Protection against cyberattacks
Development of risk management systems	Threat monitoring and risk assessment	Timely response to crisis situations
International cooperation	Joint programs with the EU and NATO	Exchange of experience and improved security levels

e-ISSN 2786-5533

Development of backup energy systems	Creation of alternative energy supply sources	Enhanced energy resilience

Source: compiled by the author based on [11–14].

The analysis of the directions presented in the table indicates that the effective protection of critical energy infrastructure requires a comprehensive approach that integrates the modernization of energy systems, the development of cybersecurity, and the strengthening of international cooperation in the field of energy security. The implementation of these measures will enhance the resilience of energy networks to contemporary threats and ensure the stable functioning of the national energy system.

Conclusions. Critical energy infrastructure under contemporary conditions is acquiring a system-forming role within the national security framework of the state, as its stable functioning ensures the continuity of economic processes, the operation of public authorities, and the overall functioning of society. The intensification of threats caused by the full-scale war objectively transforms approaches to understanding its role, shifting the focus from maintaining basic functionality to strengthening the resilience of energy systems under conditions of continuous disruptive impact. In this context, disruptions in the operation of energy facilities are no longer viewed solely as technical issues but as factors exerting a multidimensional impact on economic stability, social security, and the defense capacity of the state.

The regulatory and legal framework established in Ukraine has laid the institutional foundations for the protection of critical infrastructure; however, the evolving nature of contemporary threats highlights the need for its further development and adaptation to new security conditions. The growing influence of military factors, the intensification of cyber threats, and the accumulation of industrial risks necessitate the improvement of security management mechanisms oriented toward prevention, flexibility, and rapid recovery. This transformation involves a transition from fragmented measures to an integrated risk management system capable of ensuring a comprehensive response to interrelated threats.

In this regard, the application of international experience becomes particularly important, as it demonstrates the effectiveness of systemic models

for critical infrastructure protection based on the integration of legal, organizational, and technological instruments. The practices of European Union and NATO countries confirm the importance of enhancing cross-sectoral cooperation, implementing risk-oriented approaches, and strengthening cybersecurity as an integral component of energy system security. At the same time, the increasing level of digitalization requires the parallel development of protective mechanisms capable of reducing the vulnerability of energy infrastructure to cyber incidents.

Taking this into account, the prioritization of energy network modernization, the development of backup and decentralized energy supply systems, as well as the strengthening of cybersecurity and coordination among security actors acquires strategic significance. The implementation of these directions enables the formation of an adaptive and resilient energy system capable of functioning under multidimensional threats, thereby contributing to the strengthening of national security and ensuring sustainable development of the state.

References:

1. National Security Strategy of Ukraine "Human Security – Country Security". Decree of the President of Ukraine No. 392/2020, September 14, 2020. Available at: https://zakon.rada.gov.ua/laws/show/392/2020

2. Energy Security Strategy of Ukraine. Resolution of the Cabinet of Ministers of Ukraine No. 907-r, August 4, 2021. Available at: https://zakon.rada.gov.ua/laws/show/907-2021

3. Cybersecurity Strategy of Ukraine "Secure Cyberspace as a Key to the Country's Successful Development". Decree of the President of Ukraine No. 447/2021, August 26, 2021. Available at: https://zakon.rada.gov.ua/laws/show/447/2021

4. Sytnyk, H. P., Oluiko, V. M., & Vavrynchuk, M. P. (2007). *National Security of Ukraine: Theory and Practice*. Kyiv: Kondor. Available at: https://elar.khmnu.edu.ua/items/129a6a48-0791-4333-a036-e1b01a31080d

5. Konechenkov, A. (2022). Renewable Energy Sector of Ukraine Before, During and After the War. Razumkov Centre. Available at:

https://razumkov.org.ua/statti/sektor-vidnovlyuvanoyi-energetyky-ukrayiny-do-pid-chas-ta-pislya-viyny

6. Horbulin, V. P. (Ed.). (2017). *World Hybrid War: Ukrainian Front*. Kyiv: NISS.

7. Bazyluk, Y., Vlasenko, R., Vlasiuk, O., et al. (2025). *Economic Security of Ukraine under High Military Risks and Global Instability*. Kyiv: NISS. https://doi.org/10.53679/NISS-analytrep.2025.03

8. Ksendzuk, V. V., & Pokotylo, M. Y. (2025). Energy security of Ukraine and the world: assessment of the impact of the Russian-Ukrainian war and market transformation forecasts. *Economics, Management and Administration*, 2(112), 46–53. https://doi.org/10.26642/ema-2025-2(112)-46-53

9. International Energy Agency. (2025). *World Energy Outlook 2025*. Paris. Available at: https://www.iea.org/reports/world-energy-outlook-2025

10. International Energy Agency. (2025). *Electricity 2025 – Analysis and Forecast to 2027*. Paris. Available at: https://www.iea.org/reports/electricity-2025

11. OECD. (2019). *Good Governance for Critical Infrastructure Resilience*. Paris: OECD Publishing. https://doi.org/10.1787/02f0e5a0-en

12. European Union Agency for Cybersecurity (ENISA). Energy. Available at: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy

13. North Atlantic Treaty Organization (NATO). Energy security. Available at: https://www.nato.int/en/what-we-do/wider-activities/energy-security

14. NATO Energy Security Centre of Excellence. (2023). Vilnius. Available at: https://www.enseccoe.org

15. Law of Ukraine "On Critical Infrastructure" No. 1882-IX, November 16, 2021. Available at: https://zakon.rada.gov.ua/laws/show/1882-20

16. Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" No. 2163-VIII, October 5, 2017. Available at: https://zakon.rada.gov.ua/laws/show/2163-19

17. Biriukov, D. S., Kondratov, S. I., Nasvit, O. I., & Sukhodolia, O. M. (2015). *Green Paper on Critical Infrastructure Protection in Ukraine*. Kyiv: NISS.

Available at: https://niss.gov.ua/sites/default/files/2015-12/Green%20Paper%20-%20dopovid.pdf

18. Kovalov, K. Y. (2025). Modern challenges and threats to critical infrastructure of Ukraine under martial law. *Private and Public Law*, 1, 75–80. https://doi.org/10.32782/2663-5666.2025.1.12

19. National Institute for Strategic Studies. (2017). Threats to critical infrastructure and their impact on national security. Available at: https://www.niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zagrozi-kritichniy-infrastrukturi-ta-ikh-vpliv-na-stan-nacionalnoi

20. Government of Ukraine, World Bank, European Commission, United Nations. (2026). *Ukraine – Fifth Rapid Damage and Needs Assessment (RDNA5)*. Available at: https://www.undp.org/ukraine/publications/ukraine-fifth-rapid-damage-and-needs-assessment-rdna5-february-2022-december-2025

21. International Energy Agency. (2025). *Ukraine's Energy Security: A Pre-Winter Assessment*. Paris. Available at: https://www.iea.org/reports/ukraines-energy-security

22. International Energy Agency. (2024). *Ukraine's Energy Security and the Coming Winter*. Paris. Available at: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter

23. United Nations Ukraine. (2023). *Ukraine Energy Damage Assessment (Executive Summary)*. Available at: https://ukraine.un.org/en/226424-ukraine-energy-damage-assessment-executive-summary

Funding. This research received no external funding.

Use of AI. AI was not used in the preparation of this manuscript. The author bears full responsibility for the content of the article.

Acknowledgments. The author declares no acknowledgments.

Received: 12.04.26
Accepted: 27.05.26
Published: 26.06.26