POLITYKA ENERGETYCZNA – ENERGY POLICY JOURNAL

2025 ✦ Volume 28 ✦ Issue 1 ✦ 55–76

DOI: 10.33223/epj/193724

Dmytro Beseda[1], Yurii Bidiuk[2], Olena Kravchenko[3], Mykola Pogrebytskyi[4], Dmytro Shchoholiev[5]

The energy system as an object of legal regulation and implementation of innovative technologies for the protection of critical infrastructure

Abstract: The necessity to enhance and reevaluate the safety of energy infrastructure has been brought to light by the ongoing crisis in Ukraine. This paper examines the current status of the Ukrainian energy system, with particular attention paid to legislative frameworks and the possible incorporation of cutting-edge technologies for improved protection. The principal objective is to evaluate the efficacy of current legislation and suggest enhancements to ensure the safety of vital infrastructure. To do this, the study thoroughly examines Ukrainian energy laws, pointing out both the advantages and disadvantages of the existing legal system. Reviewing the laws and rules that

✉ Corresponding Author: Dmytro Beseda; e-mail: besedadmytro@ukr.net

[1] National Academy of Security Service of Ukraine, Ukraine; ORCID iD: 0009-0005-0628-2605; e-mail: besedadmytro@ukr.net

[2] National Academy of Security Service of Ukraine, Ukraine; ORCID iD: 0009-0002-0515-7050; e-mail: y_bidiuk@meta.ua

[3] National Academy of Security Service of Ukraine, Ukraine; ORCID iD: 0000-0003-0246-1022; e-mail: olkravchenkoo@meta.ua

[4] National Academy of Security Service of Ukraine, Ukraine; ORCID iD: 0000-0003-0779-6577; e-mail: myk.pogrebytskyi@ukr.net

[5] National Academy of Security Service of Ukraine, Ukraine; ORCID iD: 0009-0009-5005-1045; e-mail: dmshchoholiev@meta.ua

guarantee energy facilities' lawful operation and operational integrity is part of the investigation. By examining several theoretical perspectives on the notion of the „energy system," the research develops a thorough definition and pinpoints the essential elements and traits of the system. The study examines the requirements for vital infrastructure, setting the energy system apart from the more significant fuel and energy industry. The criticality levels and the responsibilities of the relevant authorities in overseeing these infrastructures are assessed in the study. A study of international documents also emphasizes how critical it is to uphold established norms and mitigate any risks that energy infrastructure may encounter.

Keywords: artificial intelligence, cybersecurity, cascading effects, sectoral body, national interest

Introduction

In the context of martial law, the protection and improvement of regulatory regulation of energy system facilities has become particularly relevant to the potential risks and threats faced by the energy sector. There are certain external factors that should be considered when studying this topic, including the potential for physical and information damage to critical energy infrastructure and its vulnerability to cyberattacks, which are becoming more dangerous over the years. The problem of implementing various innovative technologies in the energy system remains the main factor that can affect the level of protection of the mechanism. Still, insufficient study of the legislative regulation of this process complicates the adaptation of the facilities in question to modern challenges.

The imperfection of legal regulation of critical infrastructure facilities results in the absence of a transparent system of protection, particularly for energy facilities (Yefimenko et al. 2023). This topic was studied in the works of Bohdan (2022), Bielai and Lavrov (2023), who insisted on specifying and improving legislative activities as a key factor in protecting such facilities. The authors of the study noted that security organization, in this case, also involves optimizing the coordination and management of the authorities responsible for the energy system and strategic regulation of innovation processes. At the same time, the situation of sectoral bodies in the field of critical infrastructure protection, which, according to the current legislation, are responsible for monitoring these phenomena and the vector of development in this direction, is still unexplored.

Innovative technologies are one of the most influential means of improving the protection of critical infrastructure facilities, which creates the need to find ways to apply them. Studies were conducted in the works of Slobodian et al. (2022) and Zyhrii et al. (2023), which described the key principles of state policy for regulating innovations that should be considered in the regulatory framework. Moreover, the authors studied the future consequences of the use of technology in various spheres of public life, which determined the need for flexibility and balance in legal regulation, especially in regulating critical energy infrastructure. However, it is worth noting that

examples of specific applications and a list of potential types of innovative technologies that can be implemented in the energy system remained outside the scope of these studies.

To implement the protection system, it is not enough to formally enshrine specific desired outcomes in law, so it is necessary to develop their clarification in the form of specific mandatory measures at the level of, for example, by-laws to ensure the realization of the ultimate goal. Thus, in the research of Krikun (2021), Plahotniuc (2022), the authors studied the optimal combination of coordination and incentive methods to promote the implementation of critical infrastructure security measures. In particular, the authors found that the forms and methods of protecting critical infrastructure are key components of the administrative and legal mechanism, and their interconnection is revealed through organizational and legal operations. On the other hand, the legal regulation of managerial and technical means at critical infrastructure facilities in the domain of cyber defense, which is within the scope of authority of managers and owners of such structures, is unexplored.

The stable functioning of critical energy system facilities is an essential factor for ensuring national security, and therefore, formalizing their importance is an integral part of public policy, which includes specifying the position of innovative technologies in this system. The problem raised in the works of Sukhodolia (2022), Mashtaliar et al. (2023), the authors highlighted the importance of introducing the latest strategies and technologies to protect the energy system and respond to new threats, which should ensure the sustainability of society. Such measures should include predictive threat analysis, the use of the latest technologies, the creation of integrated protection strategies, and the implementation of international standards. The study also examined some areas of artificial intelligence (AI) technology used in the energy sector, which identified the priority of strategic planning. While agreeing with this statement, it should be noted that even though AI is the most popular innovative technology in the current system of critical energy infrastructure, alternative tools, such as the Internet of Things (IoT) or blockchain, have not been considered. In addition, the issue of adapting AI to martial law remains unaddressed.

Therefore, based on the scientific developments in the chosen topic, it should be noted that the study was aimed at a legal analysis of the situation of the objects that form the energy system, which should take into account current trends in the form of innovative technologies that can be used to improve their protection system. The research objective was to study the legal acts regulating this area of relations. Another area of activity was to identify the general organizational and technical requirements and measures to be implemented as part of the operation of critical energy infrastructure in the field of cyber defense. The third task was to formulate a list of types of innovative technologies that are already in use or could potentially be used to improve the protection of energy system facilities.

1. Materials and methods

During the study, the authors examined the legal acts related to the functioning of the energy system and ensuring its sustainability and reliability. To implement the above, the method of interpretation of legal norms was used, which also contributed to the specification of their legal status and the definition of legal regulation mechanisms by studying the current state of legislation. This interpretation helped to identify areas where innovative approaches could be introduced to improve the critical infrastructure protection system in the energy sector. In general, this way, the meaning of the provisions of the energy system contained in various legal acts was determined, which forms an inseparable link between them.

The study was significantly influenced by the analysis of national and foreign documentation related to energy security and critical infrastructure protection based on the formal legal approach. This method was used to systematically examine the legislation governing the functioning of the energy system and identify legal provisions related to the protection of critical facilities. This approach made it possible to formulate potential areas of development and build a general outline of the legal system for regulating energy facilities as part of critical infrastructure.

Building an understanding of the legal status of critical energy infrastructure is impossible without substantiating the concept of the "energy system" itself as a phenomenon containing various elements that, in their interaction, ensure the functioning of the entire mechanism. In this area, the study considered theoretical approaches and developments from different fields of knowledge, which, among other things, required the use of existing theoretical developments of competent scientists. Moreover, the researchers' scientific works contributed not only to establishing the terminological boundaries of the concept of "energy system" but also to the applied identification of ways to improve their protective mechanisms by introducing innovative technologies.

The bulk of the materials used in the study were based on the national legislative framework that regulates the operation of critical energy infrastructure facilities, defines the activities of the bodies responsible for monitoring the list of such facilities, formulates the measures to be taken in such structures; and identifies the criteria that these components of the mechanism must meet. The Law of Ukraine No. 1882-IX "On Critical Infrastructure" (2021) has proved to be one of the most popular legal acts, containing a significant share of general and special provisions that affect energy facilities and the entire critical infrastructure.

The application and understanding of some provisions of the above-mentioned law is impossible without by-laws that clarify its meaning and serve as a guideline for implementing specific provisions. For example, the following should be mentioned: Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-p "On Some Issues of Objects of Critical Infrastructure" (2020), Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p "On the Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects" (2019) and Resolution of the Cabinet of Ministers of Ukraine No. 943-2020-p "On Some Issues of Objects of Critical Information Infrastructure" (2020). The norms contained in these by-laws were used

to determine the procedures for classifying a facility as critical infrastructure and formulate the principles of the cyber defense system, which should be ensured, in particular, by the owners or managers of such facilities.

It is also worth mentioning the Agreement to the Energy Charter (1994) and EU-NATO Task Force "On the Resilience of Critical Infrastructure" (2023), which, as international documents, should serve as a guide for legislators in the field of energy legislation. In the study, these materials were used to assess international cooperation and coordination principles and determine the consequences of potential threats to the functioning of the energy system.

2. Results

2.1. Concept and characteristics of an energy system

Generally, the energy system combines physical and social components that provide society access to various energy sources necessary for its vital activity. The main task of this complex is the production, transmission, distribution, and consumption of energy, which is realized by the interaction of all system components. Within the framework of the study, these components were called "elements", which at the same time form stable independent objects of legal regulation and in their totality, explain the existence of such a mechanism as the energy system (Table 1).

Table 1. Components that ensure the functioning of the energy system

Tabela 1. Elementy zapewniające funkcjonowanie systemu energetycznego

Element name	Element structure
Energy sources	Sources that produce energy. They may include coal, oil, gas, nuclear fuel, wind power, solar power, hydroelectric power, and others.
Production facilities	Power plants and other production facilities that convert energy from various sources into electrical, thermal or mechanical energy.
Transmission and distribution networks	Systems and infrastructure that transport energy from production facilities to end users through electricity, gas, oil, and other types of networks.
Transport infrastructure	Systems and networks that transport energy, such as oil, gas or coal, from the point of extraction to the point of use or processing.
Energy storage systems	Various technologies and facilities used to store energy for future use, such as batteries, pumped storage, and thermal storage.
Energy consumers	Enterprises, residential buildings, vehicles and other facilities that use energy for production, lighting, heating, cooling and other purposes.
Management and control systems	Technologies and software used to monitor, control and optimize the operation of the energy system to improve its efficiency and reliability.

Source: compiled by the authors based on Law of Ukraine No. 2019-VIII "On the Electricity Market" (2017).

There are various ways to comprehend the idea of the energy system, depending on the context of the relations being studied. According to the economic approach, the mechanism being studied is a financial system governed by market forces. This viewpoint highlights how crucial economic variables are to the operation of the energy system, including supply and demand, energy prices, and other variables. According to sociologists, the energy system impacts both individual lives and society. This strategy focuses on social issues such as social justice, energy poverty (i.e., lack of access to energy services), and consumer access to energy.

The most similar to the definition proposed at the beginning of the study is the understanding of the energy system in the context of the systems approach, which explains this structure as a set of interconnected elements (power plants, power grids, distribution systems, consumers), which are interdependent and work together to ensure uninterrupted electricity supply. Finally, the legal approach, primarily based on the norms and principles of international, national, and regional legislation governing relations in the energy sector, has been identified as the most effective for interpreting the energy system concept within the study's scope (Boute 2023). According to this approach, it was proposed to define the energy system "as a set of legal and regulatory acts that regulate the status of subjects and objects of the entire mechanism, as well as the legal regime of its functioning, including the instruments for protecting this structure".

In the energy system concept and different approaches, an important aspect is the formulation of specific features, i.e., features characteristic of this object of legal regulation, which allow the legislator and scholars to regulate relations in this area properly. The most noticeable feature from the above definition is complexity, explained by various components, including energy sources (from production to distribution) and energy transmission networks. These components constantly interact with each other, contributing to forming a single system that ensures energy supply, considering demand and various technical and economic factors, allowing speaking of such a characteristic as integration. The ability to continuously provide a reliable and uninterrupted energy supply to meet the needs of consumers in all conditions, including emergencies and fluctuations in demand, is a separate feature that has been called the stability of the energy system. The most optimal use of resources and technologies to ensure high productivity and minimize losses during energy production, transportation, and distribution can be identified as a separate characteristic that measures the mechanism's efficiency.

The security attribute materializes the technical and information protection of systems from potential threats, such as cyberattacks, natural disasters, or technical incidents that could lead to disruptions in the functioning of the system. In other words, this attribute explains the importance of preventing the creation of dangerous situations, their prompt detection, and effective resolution in the event of their occurrence. The last feature was identified as the sustainability of innovation, which indicates the possibility of adapting and integrating the latest technologies and management methods to improve the energy system's efficiency, economic feasibility, and sustainability.

2.2. Energy system as an object of legal regulation

The energy system is one of the most essential components of the critical infrastructure of any country, as the continuous operation of electricity grids, gas pipelines, and other energy networks is a key element for ensuring a high standard of living and economic development. In this regard, it is essential to emphasize that legal regulation in the energy sector is of great importance, as it aims to ensure the stability, security, efficiency, and sustainable development of this system. The legal regulation of the energy system is carried out at various levels, primarily international and national. At the global level, international treaties and conventions are adopted to regulate cross-border energy transportation, environmental protection, nuclear energy safety, and other issues. At the national level, laws and other regulatory acts are adopted that regulate the activities of energy market players, set energy tariffs, and stimulate the development of alternative energy sources. The specific goals should be achieved as part of improving the regulatory framework for this structure. Thus, firstly, the legislator should be guided by the following benchmarks: ensuring the country's energy security, developing competition in the energy market, attracting investments in the energy sector, improving energy efficiency, and protecting the environment.

The Law of Ukraine No. 2019-VIII "On the Electricity Market" (2017) is one of the fundamental legal acts regulating the concept of the "energy system." This Law contains the bulk of terms and regulates issues in the electricity sector. In particular, it includes the idea of electricity, understood as energy produced at electricity facilities and intended for commercial trade. Equally importantly, the act explains the definition of the "integrated energy system of Ukraine," which, according to this provision, should be interpreted as a complex of power plants, power grids, and other electricity infrastructure facilities that are centrally managed and jointly coordinate the production, transmission, and distribution of electricity. The Law also specifies the definition of critical energy infrastructure, characterized as a set of facilities that play a vital role in society, ensuring its functioning and well-being. The inoperability or destruction of such facilities can have a profound impact on national security and defense, as well as have negative consequences for the environment or lead to severe financial losses and casualties among the population (Akani 2023; Shchokin et al. 2023).

An understanding of the legal position of the energy system in modern national legal practice is also included in the content of Law of Ukraine No. 1882-IX "On Critical Infrastructure" (2021). Russia's full-scale invasion of Ukraine has created a particular relevance around this topic, as the facilities regulated by the Law are among the key military targets of the aggressor country. In addition, it is impossible to ignore the public outcry and numerous references to this topic in the media. Still, the question of understanding "critical infrastructure facilities" in the legal sense arises. Thus, according to Law of Ukraine No. 1882-IX (2021), a critical infrastructure facility is considered to be an integral infrastructure element, system, and complex, which is crucial for the economy, national security, and defense, and damage or disruption of their operation may have serious consequences for vital national interests. Accordingly, critical infrastructure should be understood as the total number of all objects that fall under the above definition.

However, defining a critical infrastructure facility using only one definition is impossible. Therefore, Article 8 of Law of Ukraine No. 1882-IX (2021) provides that the classification of this category should be based on a set of criteria that reflect their importance in the social, political, economic, and environmental contexts for the protection of the country the security of citizens, society, and the state, as well as for ensuring Law and order. These criteria take into account the pivotal significance of the facilities in providing vital functions and services, indicate the existence of threats to them, and the likelihood of creating crises due to various factors (e.g., illegal interference with their activities, obstacles to their smooth functioning, natural disasters, human influence); and the time required to restore normalcy after such events.

Speaking about the criteria themselves, the content of Law of Ukraine No. 1882-IX (2021) suggests the existence of the following:

- the likelihood of causing significant damage to the expected life of the population;
- the vulnerability of the facilities and the severity of the possible negative impact;
- the emergence of challenges and threats that may arise about critical infrastructure facilities;
- the extent of negative consequences for the state that affect the operation of strategically essential facilities and may lead to the loss of nationally significant assets;
- fulfillment of goals aimed at realizing vital national interests;
- impact on the operation of other critical infrastructure sectors;
- the time required to eliminate the negative consequences and their future impact on the state's activities in other areas of state functioning.

The adoption of Law of Ukraine No. 1882-IX (2021) was accompanied by the approval of three by-laws by the Cabinet of Ministers, namely Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p "On the Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects" (2019), Resolution of the Cabinet of Ministers of Ukraine No. 943-2020-p "On Some Issues of Objects of Critical Information Infrastructure" (2020) and Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-p "On Some Issues of Objects of Critical Infrastructure" (2020). In addition, the Concept of ensuring the cybersecurity of critical infrastructure in the energy sector, developed by the Ministry of Energy, was approved. Still, it was never adopted due to objective factors, which primarily involved the outbreak of a full-scale war.

Regarding the by-laws mentioned above, it is necessary to say that the Resolution of the Cabinet of Ministers of Ukraine No. 943-2020-p (2020) regulates issues related to critical information infrastructure, while the other two directly regulate matters related to the energy sector. The Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-p (2020) included a special Procedure that systemizes and implements a mechanism designed to ensure the procedure for classifying a particular object as critical infrastructure, as well as provides for the division of all elements into sectors, which is specified in the approved List, which is part of the Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-p (2020). According to the procedure set out in the Resolution, responsible structures should be established in the form of sectoral bodies in the field of critical infrastructure protection, which are responsible for categorizing and identifying all objects falling under the above List to standardize and unify their activities, all their decisions should be subject to the criteria set out in a specially developed Methodology.

It is essential to note that the provisions set out in Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-p (2020) are consistent with Article 10(2) of Law of Ukraine No. 1882-IX "On Critical Infrastructure" (2021), which provides for the division of all critical infrastructure into four categories of criticality, including units belonging to the energy system. Based on this rule, the first category of criticality should be considered to be those that are particularly important and of strategic importance for the entire state. Their disruption can cause serious problems for other key infrastructure facilities and lead to a crisis at the national level. The objects of the second category of criticality are vital and of great importance for a particular region. Problems in their operation can cause an emergency limited to a geographical area. Facilities of the third category of criticality include those significant at the local level. Disruptions in their operation could lead to a crisis limited to a particular community. The fourth criticality category consists of elements necessary for specific regional needs and may cause a crisis limited to a certain local level.

The current legislation's position on the energy system is specified in the previously mentioned Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-p (2020), where this structure is referred to as sector number one, called "Fuel and Energy." In addition to the division into sectors, the List provides for a more detailed classification into sub-sectors, each of which must provide the services allocated to them. Thus, the following sub-sectors can be said to exist: electricity, coal mining, peat extraction, oil industry, nuclear energy, and power engineering. The services they provide can be summarized as the extraction of materials, transmission of minerals, storage, production of special equipment, distribution of electricity, and operation of structures, wires, and systems for various purposes. The Ministry of Energy is designated as the responsible sectoral authority in the field of critical infrastructure protection of the energy system. To assess whether the designated structure is correct, the relevant Resolution of the Cabinet of Ministers of Ukraine No. 507-2020-p "On Approval of the Regulation on the Ministry of Energy of Ukraine" (2020) was studied, which specifies its two main areas of activity: organization and implementation of strategic management in the areas of electricity, nuclear and coal industry, peat extraction, oil and gas and oil and gas processing complex, as well as the establishment and implementation of the state strategy in the field of renewable energy sources and alternative forms of gas fuel, and establishing and implementing a state strategy for the use of renewable energy sources and alternative forms of gas fuel, and ensuring control over the electricity, heat, and natural gas sectors. Based on these regulated objectives of the Ministry of Energy, it is difficult to disagree that this body is the most competent and specialized in the issues to be resolved by the procedures set out in the content of the analyzed Resolution of the Cabinet of Ministers of Ukraine No. 507-2020-p (2020).

The other mentioned Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p "On the Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects" (2019) was created to regulate issues related to ensuring proper cyber protection of critical infrastructure facilities. This by-law regulates general requirements that should provide the conditions for organizational, methodological, technical, and technological support for the cyber defense of critical infrastructure facilities. All the requirements listed therein must be strictly

observed by enterprises, institutions, and organizations classified as essential infrastructure facilities under the law, including energy system structures.

Returning to the Law of Ukraine No. 1882-IX (2021), it is not worth ignoring the provision enshrined in Article 9, paragraph 2, part 4, which refers to energy supply, including heat supply, as a function whose violation can potentially lead to adverse consequences for the national security of the entire country. This provision identified specific areas of state activity that may be affected by breaches in the energy supply sector. First and foremost, it is about economic sustainability, which means the availability of a stable and reliable energy supply, which is an essential condition for the functioning of industry, transport, agriculture, and other sectors of the economy. On the other hand, the security situation will be threatened, which may manifest in a lack of energy, creating a crisis for the defense forces and transport. In a global sense, the possibility of dependence on imported energy sources is one of the alternative scenarios, which will lead to vulnerability to external influences and political risks. Of course, social stability will be objectively affected, as a reliable energy supply is essential for the comfort and safety of citizens, especially during the cold season when heat is essential for heating homes and ensuring comfortable living conditions. The last argument is the strategic importance of the energy sector, including the use of domestic resources and the development of alternative energy sources, which contribute to the country's more independent and competitive position in the global energy market (Costa et al. 2023).

The role of international documents in the energy sector has been identified as an essential component of legal regulation, the importance of standardizing standard requirements at the global level, the need to ensure the efficiency and stability of legal regulation of the energy sector, and to improve cooperation and coordination between countries. In this context, the Energy Charter Agreement (1994) is a fundamental document in international energy cooperation. This document covers a wide range of issues related to energy security, including energy transit, energy investment, and environmental protection. Moreover, Article 3 sets out the basic principles that should guide the participating countries in formulating their energy policies, which include:

- improving the functioning of market mechanisms, including market-oriented pricing and better consideration of environmental costs and benefits;
- reducing barriers to energy efficiency, which encourages capital investment;
- development of fundraising tools for energy efficiency initiatives;
- providing education and public awareness in this area;
- increasing the transparency of the legal and regulatory framework;
- dissemination and exchange of technologies.

A deeper understanding of the current state of energy security was explored based on the Report of the EU-NATO Task Force "On the Resilience of Critical Infrastructure" (2023), which states that the proper functioning of the global and societal systems is subject to many factors, one of which is the unimpeded and efficient supply of energy from various sources. Thus, based on the EU-NATO Task Force (2023), the study concluded that energy security is becoming increasingly complex in the current geopolitical context as EU-NATO adversaries and strategic competitors engage in malicious activities in cyberspace, manipulate energy supplies, and use

economic pressure. In addition, the EU-NATO Task Force (2023) identifies unique features that require special measures to ensure resilience, namely real-time requirements, cascading effects, and technology mix. The first feature means that some energy systems must respond to challenges instantly and cannot tolerate processing delays. Cascading effects can lead to a chain reaction during a large-scale disruption, quickly depriving consumers in different countries and sectors of access to electricity (Knapik 2019). The latter feature indicates the obsolescence of technologies and infrastructure, which have a lifespan of 30 to 60 years and, therefore, require parallel and timely innovation and digitalization.

The nation's energy infrastructure is under tremendous strain due to the ongoing crisis in Ukraine, underscoring its susceptibility to physical and cyber-attacks. The fact that hostile forces have targeted energy installations on purpose has highlighted the urgency of immediately improving safety precautions. As part of the national defense strategy, the conflict has expedited the adoption of cutting-edge technologies. AI and IoT are being used to monitor and safeguard vital infrastructure in real time. Nonetheless, the conflict has also brought to light deficiencies in the current legal and regulatory structures concerning the synchronization of reactions to concomitant physical and cyber hazards. Ukraine has to make it a priority to quickly implement resilient technologies and make sure that the legal frameworks are updated to facilitate their efficient usage in the face of present and potential threats to reduce these risks (Volkov et al. 2023).

2.3. The energy system as an object of implementation of innovative technologies for critical infrastructure protection

Innovative technologies are a key driver of progress. Still, priorities in this area must be constantly reviewed to meet new challenges arising from the widespread deployment of renewable energy sources and the electrification of various end-use sectors, such as construction, transport, and industry. The energy system is one of the most essential components of critical infrastructure as it ensures the functioning of all other sectors of the economy and the life of the population; its protection from cyber and physical attacks is one of the most important tasks of ensuring national security (Cenușa 2022; Shahini et al. 2024). Physical protection of energy system facilities may include their fencing and access control, protection against intrusion in the form of various fortifications (safes, armored doors, windows), and the presence of security and law enforcement agencies (Semenenko et al. 2023). However, all these means were defined as "traditional" in the study to the extent of their durability and age, indicating the need to improve them and introduce alternatives, such as innovative technologies. It is worth noting that the particularly dynamic development of information technology in recent decades has necessitated the creation of an effective cyber defense system and, accordingly, the regulation of this issue at the regulatory level.

For instance, the previously mentioned Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p (2019) stipulates that cybersecurity measures and requirements are to be envisaged

and implemented at all stages of the critical infrastructure facility's life cycle. Clause 12 sets out specific areas that should ensure the organizational and technical security of the facility. In particular, the act mentions the following measures:

- setting the conditions for using external devices and storage media;
- recording of events occurring by the components of the critical information infrastructure facility and their regular verification;
- ensuring the availability and sustainability of information resources;
- establishing the conditions for the placement of facility components;
- establishing the requirements for the operation of hardware and software;
- access control for administrators and users;
- protecting the network of components and information resources;
- identification of administrators and users.

Each of the above measures is specified in a special List of requirements for each of the above areas, which was approved by the same Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p (2019), which must be observed by each owner or manager of a critical infrastructure facility in organizing its workflow. On the other hand, introducing specific innovative technologies in the cyber defense system is an undeniable advantage for implementing the above measures. For example, the technologies mentioned in Table 2 have several potentially beneficial effects, including increased resilience of the power system to cyber and physical attacks, improved efficiency of power system management, reduced energy costs, and increased reliability of power supply.

Table 2. Types of innovative technologies for critical infrastructure protection

Tabela 2. Rodzaje innowacyjnych technologii ochrony infrastruktury krytycznej

Name of the innovative technology	How to implement it
Artificial intelligence	It can be used to analyse data on the operation of the power grid to identify anomalies and potential threats. Another application is automatic response to cyberattacks and other emergencies.
Internet of Things	IoT devices can be used to collect real-time data about the state of the power grid. This data can be used to monitor and predict potential problems, and to make decisions about how to manage the grid.
Blockchain	It can be used to create a secure and transparent energy system management system, as well as to track the origin of energy and prevent data falsification.
Quantum computing	They can be used to develop new cryptography methods that are resistant to attacks by quantum computers.

Source: compiled by the authors.

Among the innovative technologies listed in Table 2, AI was identified as the most widespread and relevant. In the current Ukrainian legislation, the definition of this technology is contained in Order of the Cabinet of Ministers of Ukraine No. 1556-p "On the Approval of the Concept of

the Development of Artificial Intelligence in Ukraine" (2020), according to which it should be understood as a system of information technology that is organized in such a way as to perform complex tasks using scientific research methods and information processing algorithms. This system works with information obtained in work or independently created and uses its own knowledge bases, decision-making models, and information processing algorithms to achieve its goals.

The practical application of AI can be realized in the form of automatic processing of the state of technical equipment of energy facilities; approximate forecasting of the dynamics of the cost of energy resources based on demand and taking into account energy consumption; prediction and analysis of the impact of weather conditions on potential changes in the production mode, which should affect the increase or decrease in the level of efficiency of such a structure (Kunskaja et al. 2023; Zarichuk 2023). At the same time, the study took into account the specifics of the energy system as part of critical infrastructure, and therefore, at the current stage, the capabilities and capacities of AI should be aimed at developing a plan for the redistribution of energy resources, taking into account the potential danger of threats from the aggressor country, whose goal is to deliberately damage energy facilities to create obstacles to their regular operation.

AI can also evaluate enormous volumes of grid data to identify anomalies and possible risks quickly. AI systems, for example, can automatically redirect energy flows to avoid disturbances and isolate impacted network portions in response to cyberattacks. By examining trends in operating data, AI can also be used to anticipate equipment breakdowns, enabling preventive maintenance and lowering the likelihood of unplanned outages. IoT devices can also offer ongoing energy infrastructure monitoring, transmitting data in real-time to centralized systems that leverage AI to optimize energy distribution and improve security protocols. Blockchain technology provides a safe way to handle energy-related transactions, guaranteeing openness and thwarting illegal access to vital systems. Even though it is still in its infancy, quantum computing has the potential to completely transform the cryptographic techniques used to safeguard energy infrastructure against sophisticated cyberattacks (Kidalova 2020; Vliamos 2024).

Numerous obstacles exist in integrating blockchain, IoT, and AI technologies into the energy system. These include expensive expenses, substantial data infrastructure requirements, and the possibility of relying too much on AI. Additionally, specialized workers are needed, necessitating a significant investment in education and training. The regulatory environment must accommodate technological improvements without sacrificing security. Government, business, and academia must cooperate to create and execute practical solutions.

According to the report, many different rules and regulations work together to maintain the stability and security of the Ukrainian energy system, making its legal framework intricate and multidimensional. However, the analysis shows that even if the current framework is effective at identifying essential infrastructure and allocating duties, it still needs to upgrade and incorporate cutting-edge technologies, especially in physical security and cybersecurity. Certain technologies like blockchain, IoT, and AI can significantly improve the system's resilience. The report also emphasizes the necessity of a more thorough regulatory strategy that would codify these technologies into law and offer precise instructions for how they should be applied at

various critical infrastructure tiers. Furthermore, the geopolitical environment of today has made it necessary for these technologies to be quickly adjusted to counter new threats, especially those associated with cyberwarfare and focused physical attacks on energy infrastructure.

3. Discussion

The study made it possible to identify the legislator's current approach to the legal regulation of the energy system in accordance with the current legislation and to find out the existing technological developments that can improve the protection of this mechanism as a critical infrastructure facility, using Ukraine as an example. Nevertheless, an in-depth understanding of the issues under consideration was impossible without considering the current scientific literature.

The content of the "energy system" concept can be based on different approaches (economic, legal, social), and all of them contribute to improving the perception of this mechanism, considering different sectors. For example, del Guayo (2023) considered a legal approach based on the energy system's relationship between energy law and energy justice. In the author's opinion, the relationship should be based on norms that should not act as an obstacle but as a valuable tool for achieving the goals of justice, sustainable development, and protection. It should be highlighted, therefore, that N. del Guayo did not discuss the significance of each element's qualitative interaction and structural integration at the normative level. This fact was also considered by Viñuales (2022), who thought at the theoretical level the impact of environmental changes, in particular, in particular global warming, on international and regional energy law. In this aspect, the work correlates with the study in terms of the fact that introducing innovative technologies can contribute to developing the system's response to potential weather changes and eliminating associated risks.

In the framework of the study, the systemic nature of energy infrastructure facilities was explained, among other things, by a set of legal acts and by-laws of both international and national importance that regulate relations in this area. In the works of scientists Roman and Cygańczuk (2022), the authors confirm this thesis by first analyzing Law of Poland No. 590 "On Crisis Management" (2007), which encompasses general information on the bodies competent in crisis management, their tasks, and principles of activity in this area, and specifying the provisions relating to the protection of critical infrastructure included in various regulations covering various regions of the country's activity, such as energy production and trade, defense tasks of enterprises. However, the study shows that in Ukraine, the legislation is more general, and their clarification is accompanied by the adoption of resolutions that serve as a kind of instruction. Another work supporting the fact mentioned above is the study by Obrenović (2022), which examines the harmonization of Serbian legal regulation of security plans, including energy plans, with similar European standards. Thus, it is worth mentioning the previously analyzed

Energy Charter Agreement (1994), which should be one of the key means of standardization and adaptation of legal regulation of the energy system.

The study identified two main areas of critical infrastructure protection: physical and cyber defense. The opinion of Kruszka et al. (2022) coincides with the results obtained, which determine that damage to critical energy infrastructure due to criminal activity or natural disasters can have serious consequences both at the national and international levels. However, the focus of the researchers was on the physical protection of critical infrastructure, which did not cover all the specifics of the topic, the significant influence of innovative technologies on the modern operation of energy facilities. On the other hand, in the work of Trifunovic (2024), the author took into account the peculiarity of Russian aggression against Ukraine on the functioning of critical infrastructure facilities, including physical threats and cyber-attacks. In contrast to the above study, it should be noted that the results obtained showed the importance of cyber defense at all stages of the life of an energy facility, which special measures should accompany.

The introduction of information technology and the large-scale integration of small-scale energy resources are increasing the complexity and criticality of the energy system, making it more vulnerable to physical threats and cyberattacks (Quraishi et al. 2024; Nesterov 2023). Alskaif et al. (2023) considered potential technological and digital design solutions that could reduce the impact of these threats and increase the resilience of energy systems, while Kruszka and Muzolf (2022) specified that such risks could cause severe economic losses for the state. However, according to these studies, it is not clear what criteria should be used to assess the risk of damage to a particular critical energy infrastructure facility, such as the vulnerability of system facilities, the size of potential negative consequences, and the time to eliminate them. It is worth mentioning the work of Lauf et al. (2024), which focused on the increased vulnerability of energy system facilities, which requires improving the mechanisms for protecting critical energy infrastructure. It should be clarified that, according to the study results, the most effective means of improvement are currently various innovative technologies.

Currently, AI is one of the most advanced and popular innovative technologies, which can be justified by its relative ease of use and high level of efficiency, so its implementation in the energy system is a necessity (Ostudimov and Kaminska 2023). Thus, the studies by Adewusi et al. (2024) and Yu (2024) analyzed the role of AI in the development of critical infrastructure and its impact on national security and economic stability. To be more specific, in the researcher's work, AI was defined as a separate critical infrastructure object, given its potential importance for establishing national security. However, it isn't easy to agree with the proposed statement, as the study shows that AI plays a supporting function and can be used to improve the protection of the energy system, in particular. It is also worth mentioning the detailed study by Abdelghani (2021), which aims to consider AI in cybersecurity and protection of critical infrastructures, such as the gas pipeline system, electricity grid, electricity generation, and others, which are of great importance for the security of national interests. Therefore, the results correlate with the opinion of the researchers that the introduction of AI significantly expands the ability to protect critical infrastructure.

The systematization and collection of data to optimize the management of energy facilities can be carried out through innovative technology like the IoT. This specificity was elaborated in the work of Momeni et al. (2023), which proposes the introduction of a simple, secure, and energy-efficient authentication protocol with the establishment of a session key. According to the authors, such a protocol preserves the user's anonymity to protect their privacy. Still, regarding employees performing their functions and collecting information through the IoT, it isn't easy to agree with introducing this principle to the entire mechanism. The potential of the IoT and blockchain technology merger was studied in the work by Hexmoor and Maghsoudlou (2024), which, in conformity with the authors, opens up great opportunities for improving security, transparency, and efficiency. This study reflects a forward-looking proposal that indicates ways to integrate these technologies to create a reliable, scalable, and secure infrastructure for future IoT applications, including their use to improve the protection of critical energy infrastructure. This perspective aligns with the study's findings, which also mentioned AI and quantum computing, as the integrated use of innovative technologies will help maximize their effectiveness.

Improving the cyber defense mechanisms of energy-critical infrastructure is possible only with a sustainable, strategic, and effective state policy. A review of the legislator's legal approaches in this area was carried out in the study by Ziętara (2024), which examined the issues of restoring the mechanism for protecting Ukraine's infrastructure as a result of Russian aggression, which should be subject to the legal standards of the European Union. The author also considered changes in Polish and international legislation on protecting critical infrastructure. Still, he did not believe in the essential circumstance of legal regulation of introducing innovative technologies into the energy system. Given the above and the study results, regulating the cyber defense mechanism is necessary. This statement can be supported by the work of Watney (2022) and Sanders et al. (2022), who emphasize that in the last decade, cyber threats to critical infrastructure have increased in both intensity and complexity. These works also mentioned the essential interconnectedness of infrastructure, which creates a risk of cascading consequences that could affect the economy and national security. In addition to the cascading effect in the event of damage to critical infrastructure, the study pointed to the problem of real-time requirements and the need to combine technologies due to the obsolescence of some means. Moreover, all these problems should be addressed at the legislative level to anticipate and avoid complications that may arise in the future.

Therefore, the results obtained and the studies discussed above demonstrate the importance of a comprehensive and systematic approach to the energy system as an object of legal regulation. This will ensure the quality functioning of this mechanism as part of the critical infrastructure that guarantees the welfare of the population and the economic stability of the state. The constant adaptation of critical energy infrastructure facilities to the requirements of the times necessitates taking into account innovative technologies that have a real impact on the level of protection against physical threats and cyber-attacks.

Conclusions

The report emphasizes how urgently Ukraine's energy system has to adjust its legal framework to meet contemporary difficulties, especially in light of the country's unstable geopolitical environment and rapid technical improvements. The study thoroughly comprehended the energy system by examining multiple legal documents and theoretical frameworks, characterizing its fundamental components, and classifying it as a key infrastructure. The study's main contribution is the identification of essential domains in which cutting-edge technologies like AI, blockchain, quantum computing, and the IoT can be combined to improve the security of vital energy infrastructure. The study emphasizes the importance of a well-coordinated technological and legislative framework to protect the system from offline and online threats.

According to the research, while AI has a great deal of promise for anticipating risks and maximizing the allocation of energy resources, the energy system's protection and effectiveness will be best served by an integrated strategy utilizing various technologies. The study also highlights the importance of keeping the legal framework updated to accept these developments and guarantee their successful use. The study achieved its goals by giving a thorough legal analysis of the Ukrainian energy system, emphasizing the contribution of cutting-edge technologies to its security, and making concrete suggestions for further advancements. The interactions between various technologies and how they affect the overall resilience of critical infrastructure should be investigated further.

The Authors have no conflicts of interest to declare.

References

Abdelghani, T. 2021. Implementation of artificial intelligence in the cyber security of critical infrastructures. DOI: 10.13140/RG.2.2.17485.77287.

Adewusi et al. 2024 – Adewusi, A.O., Okoli, U.I., Olorunsogo, T., Adaga, E., Daraojimba, D.O. and Obi, O.C. 2024. Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review. *World Journal of Advanced Research and Reviews* 21(1), pp. 2263–2275, DOI: 10.30574/wjarr.2024.21.1.0313.

Agreement to the Energy Charter and Final Act to it. Protocol to the Energy Charter on Energy Efficiency and Related Environmental Aspects 1994. [Online] https://zakon.rada.gov.ua/laws/show/995_056#Text [Accessed: 2024-05-22].

Akani, N.K. 2023. Analysis of the legal framework underpinning protection of critical infrastructure in armed conflicts. *Journal Jurisprudence, International Law and Contemporary Legal Issues* 17(2). [Online] https://www.rsujilclijournal.com/analysis-of-the-legal-framework-underpinning-protection-of-critical-infrastructure-in-armed-conflicts/ [Accessed: 2024-09-25].

Alskaif et al. 2023 – Alskaif, T., Pardo, M.Á.P. and Tekinerdogan, B. 2023. Energy systems as a critical infrastructure: Threats, solutions and future outlook. [In:] *Management and Engineering of Critical Infrastructures,* pp. 287–306, DOI: 10.1016/B978-0-323-99330-2.00013-1.

Bielai, S. and Lavrov, I. 2023. Theoretical foundations of the formation of the protection system of critical infrastructure facilities of Ukraine. *Honor and Law* 2(85), pp. 5–11, DOI: 10.33405/2078-7480/2023/2/85/282518.

Bohdan, B. 2022. Current issues of legal regulation of critical infrastructure protection under martial law in Ukraine. Problems of Modern Transformations. *Series: Law, Public Management and Administration* 6, pp. 46–68, DOI: 10.54929/2786-5746-2022-6-01-09.

Boute, A. 2023. Energy law and infrastructure dependencies. [In:] *Energy Dependence and Supply Security*, pp. 19–62, DOI: 10.1093/oso/9780198890478.003.0002.

Cenuşa, D. 2022. *"Reshaping" of critical regional infrastructure under the impact of war: The case of Ukraine, Russia, and the EU*. [Online] https://www.iipvienna.com/new-blog/2023/1/16/reshaping-of-critical-regional-infrastructure-under-the-impact-of-war-the-case-of-ukraine-russia-and-the-eu [Accessed: 2024-05-22].

Costa et al. 2023 – Costa, R., Krausmann, E. and Hadjisavvas, C. 2023. *Impacts of climate change on defence-related critical energy infrastructure*. Brussels: European Defence Agency, DOI: 10.2760/03454.

del Guayo, Í. 2023. Energy justice and energy law – An approach to the differences between both concepts. [In:] *The Power of Energy Justice & the Social Contract*, pp. 29–33. Cham: Palgrave Macmillan, DOI: 10.1007/978-3-031-46282-5_5.

EU-NATO *Task Force "On the Resilience of Critical Infrastructure"* 2023. [Online] https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/EU-NATO_Final_Assessment_Report_Digital.pdf [Accessed: 2024-05-22].

Hexmoor, H. and Maghsoudlou, E. 2024. IoT with blockchain: A new infrastructure proposal. [In:] *Proceedings of 39th International Conference on Computers and Their Applications*, pp. 15–24. New Orleans: International Society for Computers and Their Applications, DOI: 10.29007/htr1.

Kidalova, N.O. 2020. Legal aspects of privatization of objects of strategic importance for the economy and security of the state. *Law. Human. Environment* 11(2), pp. 169–174, DOI: 10.31548/law2020.02.020.

Knapik, M. 2019. The influence of pipe diameter selection on operating costs of heating installation in the context of the anticipated increase in electricity prices. *E3S Web of Conferences* 100, DOI: 10.1051/e3sconf/201910000034.

Krikun, V. 2021. Forms and methods of protection of critical infrastructure objects in Ukraine. *Science of European Law* 3, pp. 99–103, DOI: 10.32837/chern.v0i3.107.

Kruszka et al. 2002 – Kruszka, L., Tria, D.E., Muzolf, P. and Sobczyk, K. 2022. *Critical energy infrastructure protection: Innovative structures and materials for blast and ballistic protection*. Amsterdam: IOS Press. [Online] https://www.iospress.com/catalog/books/critical-energy-infrastructure-protection [Accessed: 2024-05-22].

Kruszka, L. and Muzolf, P. 2022. Introduction to critical energy infrastructure protection: Risks and vulnerabilities. *NATO Science for Peace and Security Series – D: Information and Communication Security* 60, pp. 1–14, DOI: 10.3233/NICSP220002.

Kunskaja et al. 2023 – Kunskaja, S., Bauer, J.F., Budzyński, A. and Jitea, I.C. 2023. A research analysis: The implementation of innovative energy technologies and their alignment with SDG 12. *Eastern-European Journal of Enterprise Technologies* 5(13(125)), pp. 6–25, DOI: 10.15587/1729-4061.2023.288396.

Lauf et al. 2024 – Lauf, J., Zimmermann, R. and Rusow, W. 2024. Energy security and critical infrastructure protection. [Online] https://www.eesc.lt/en/publication/energy-security-and-critical-infrastructure-protection/ [Accessed: 2024-05-22].

Law of Poland No. 590 "On Crisis Management" 2007. [Online] https://disasterlaw.ifrc.org/media/3464 [Accessed: 2024-05-22].

Law of Ukraine No. 1882-IX "On Critical Infrastructure" 2021. [Online] https://zakon.rada.gov.ua/laws/show/1882-20#Text [Accessed: 2024-05-22].

Law of Ukraine No. 2019-VIII "On the Electricity Market" 2017. [Online] https://zakon.rada.gov.ua/laws/show/en/2019-19 [Accessed: 2024-05-22].

Mashtaliar et al. 2023 – Mashtaliar, Y., Kozachok, V., Brzhevska, Z. and Bohdanov, O. 2023. Research of development and innovation of cyber protection at critical infrastructure facilities. *Cybersecurity: Education, Science, Technique* 2(22), pp. 156–167, DOI: 10.28925/2663-4023.2023.22.156167.

Momeni et al. 2023 – Momeni, M., Jabbari, A. and Fung, C. 2023. An energy-efficient multiple-factor authentication protocol for critical infrastructure IoT systems. [In:] *2023 7th Cyber Security in Networking Conference* (CSNet), pp. 238–242. Montreal: Institute of Electrical and Electronics Engineers, DOI: 10.1109/CSNet59123.2023.10339700.

Nesterov, V. 2023. Integration of artificial intelligence technologies in data engineering: Challenges and prospects in the modern information environment. *Bulletin of Cherkasy State Technological University* 28(4), pp. 82–92, DOI: 10.62660/2306-4412.4.2023.82-90.

Obrenović, M. 2022. Normative-legal regulation of operator security plans in the protection of critical infrastructure. *Faculty of Welfare* 1, pp. 167–181, DOI: 10.5937/fb_godisnjak0-38489.

Order of the Cabinet of Ministers of Ukraine No. 1556-p "On the Approval of the Concept of the Development of Artificial Intelligence in Ukraine" 2020. [Online] https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text [Accessed: 2024-05-22].

Ostudimov et al. 2023 – Ostudimov, B. and Kaminska, N. 2023. Energy security principles: Legal nature, classification and modernisation. *Scientific Journal of the National Academy of Internal Affairs* 28(1), pp. 55–67, DOI: 10.56215/naia-herald/1.2023.5.

Plakhotniuk, P.B. 2022. Principles and ways of enhancing cooperation between competent authorities and critical entities owned, managed and operated by private parties. *Problems of Modern Transformations. Series: Law, Public Management and Administration* 6, pp. 1–6, DOI: 10.54929/2786-5746-2022-6-01-15.

Quraishi et al. 2024 – Quraishi, A., Rusho, M.A., Prasad, A., Keshta, I., Rivera, R. and Bhatt, M.W. 2024. Employing Deep Neural Networks for Real-Time Anomaly Detection and Mitigation in IoT-Based Smart Grid Cybersecurity Systems. [In:] *3rd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics*, ICDCECE 2024. Hybrid, Ballari: Institute of Electrical and Electronics Engineers, DOI: 10.1109/ICDCECE60827.2024.10548160.

Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-p "On Some Issues of Objects of Critical Infrastructure" 2020. [Online] https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text [Accessed: 2024-05-22].

Resolution of the Cabinet of Ministers of Ukraine No. 507-2020-p "On Approval of the Regulation on the Ministry of Energy of Ukraine" 2020. [Online] https://zakon.rada.gov.ua/laws/show/507-2020-%D0%BF#Text [Accessed: 2024-05-22].

Resolution of the Cabinet of Ministers of Ukraine No. 518-2019-p "On the Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects" 2019. [Online] https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text [Accessed: 2024-05-22].

Resolution of the Cabinet of Ministers of Ukraine No. 943-2020-p "On Some Issues of Objects of Critical Information Infrastructure" 2020. [Online] https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text [Accessed: 2024-05-22].

Roman, Ł. and Cygańczuk, K. 2022. Legal dimension of the protection of critical infrastructure – Selected aspects. *Safety & Fire Technology* 59, pp. 166–181, DOI: 10.12845/sft.59.1.2022.10.

Sanders et al. 2022 – Sanders, P., Bronk, C. and Bazilian, M.D. 2022. Critical energy infrastructure and the evolution of cybersecurity. *Electricity Journal* 35(10), DOI: 10.1016/j.tej.2022.107224.

Semenenko et al. 2023 – Semenenko, O., Dobrovolskyi, U., Tolok, P., Onofriichuk, A. and Onofriichuk, V. 2023. Energy and environmental security of the European Union in the context of Russia's

unstable military and economic policy. *Scientific Horizons* 26(2), pp. 135–144, DOI: 10.48077/scihor.26(2).2023.135-144.

Shahini et al. 2024 – Shahini, E., Fedorchuk, M., Hruban, V., Fedorchuk, V. and Sadovoy, O. 2024. Renewable energy opportunities in Ukraine in the context of blackouts. *International Journal of Environmental Studies* 81(1), pp. 125–133, DOI: 10.1080/00207233.2024.2320021.

Shchokin et al. 2023 – Shchokin, R., Oliinyk, V., Amelin, O., Bondarenko, Y., Maziychuk, V. and Kyslenko, D. 2023. Methods of Combating Offenses in the Field of Ecology. *Journal of Environmental Management and Tourism* 14(1), pp. 5–15, DOI: 10.14505/jemt.v14.1(65).01.

Slobodian et al. 2022 – Slobodian, N., Levchenko, Y. and Slobodian, V. 2022. Legal regulation of the implementation of innovative strategies at the enterprise. *Ukrainian Journal of Applied Economics and Technology* 7(3), pp. 114–121, DOI: 10.36887/2415-8453-2022-3-16.

Sukhodolia, O. 2022. *Artificial intelligence in energy*. Kyiv: National Institute for Strategic Studies, DOI: 10.53679/NISS-analytrep.2022.09.

Trifunovic, D. 2024. Intelligence and protection of key (critical) infrastructure objects. [In:] *Critical Infrastructure Protection in the Light of the Armed Conflicts*, pp. 1–8. Cham: Springer, DOI: 10.1007/978-3-031-47990-8_1.

Viñuales, J. 2022. *The international law of energy*. Cambridge: Cambridge University Press, DOI: 10.1017/9781108235273.

Vliamos, S. 2024. Political Economy and Impact Assessment. *Statute Law Review* 45(1), DOI: 10.1093/slr/hmae004.

Volkov et al. 2023 – Volkov, O., Brechka, M., Stadnichenko, V., Yaroshchuk, V. and Yaroshchuk, S. 2023. The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. *Machinery & Energetics* 14(4), pp. 23–32, DOI: 10.31548/machinery/4.2023.23.

Watney, M. 2022. Cybersecurity threats to and cyberattacks on critical infrastructure: A legal perspective. *European Conference on Cyber Warfare and Security* 21(1), pp. 319–327, DOI: 10.34190/eccws.21.1.196.

Yefimenko et al. 2023 – Yefimenko, I., Sakovskyi, A. and Bilozorov, Ye. 2023. Protection of critical infrastructure as a component of Ukraine's national security. *Law Journal of the National Academy of Internal Affairs* 13(2), pp. 74–85, DOI: 10.56215/naia-chasopis/2.2023.74.

Yu, C. 2024. AI as critical infrastructure: Safeguarding national security in the age of artificial intelligence. DOI: 10.31219/osf.io/u4kdq.

Zarichuk, O. 2023. Hybrid approaches to machine learning in software development: Applying artificial intelligence to automate and improve processes. *Development Management* 21(4), pp. 53–60, DOI: 10.57111/devt/4.2023.53.

Ziętara, W. 2024. Formal and legal dimension of critical infrastructure at Polish and European level. *Annals of the Marie Curie-Skłodowska University, Section K – Political Science* 30(2), pp. 85–106, DOI: 10.17951/k.2023.30.2.85-106.

Zyhrii et al. 2023 – Zyhrii, O., Trufanova, Y., Parashchuk, L., Sampara, N. and Tsvigun, I. 2023. Law and technology: The impact of innovations on the legal system and its regulation. *Social Legal Studios* 6(4), pp. 267–275, DOI: 10.32518/sals4.2023.267.

Dmytro Beseda, Yurii Bidiuk, Olena Kravchenko, Mykola Pogrebytskyi,
Dmytro Shchoholiev

System energetyczny jako przedmiot regulacji prawnej i wdrażania innowacyjnych technologii ochrony infrastruktury krytycznej

Streszczenie

Konieczność wzmocnienia i ponownej oceny bezpieczeństwa infrastruktury energetycznej ujrzała światło dzienne w związku z trwającym kryzysem na Ukrainie. W niniejszym artykule zbadano obecny stan ukraińskiego systemu energetycznego, zwracając szczególną uwagę na ramy prawne i możliwe włączenie najnowocześniejszych technologii w celu poprawy ochrony. Głównym celem jest ocena skuteczności obowiązujących przepisów i zaproponowanie ulepszeń w celu zapewnienia bezpieczeństwa kluczowej infrastruktury. W tym celu w badaniu dokładnie przeanalizowano ukraińskie przepisy energetyczne, wskazując zarówno zalety, jak i wady istniejącego systemu prawnego. Częścią artykułu jest przegląd przepisów i zasad gwarantujących zgodne z prawem funkcjonowanie obiektów energetycznych i integralność operacyjną. Poprzez zbadanie kilku teoretycznych perspektyw pojęcia „systemu energetycznego" badanie opracowuje dogłębną definicję i wskazuje istotne elementy i cechy systemu. Praca analizuje wymagania dotyczące kluczowej infrastruktury, odróżniając system energetyczny od ważniejszego przemysłu paliwowego i energetycznego. W artykule oceniono poziomy krytyczności i obowiązki właściwych organów nadzorujących te infrastruktury. Badanie dokumentów międzynarodowych podkreśla również, jak ważne jest przestrzeganie ustalonych norm i łagodzenie wszelkich ryzyk, na jakie może natrafić infrastruktura energetyczna.

Słowa kluczowe: sztuczna inteligencja, cyberbezpieczeństwo, efekty kaskadowe, organ sektorowy, interes narodowy