DOI: 10.52363/passa-2026.1-25
UDC 323:351.746.1(477)

***Lisnyi M.**, Postgraduate Student at the National Aerospace University "Kharkiv Aviation Institute," Kharkiv*
ORCID: 0009-0008-7689-6575

***Лісний М.,** аспірант, Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків*

INSTITUTIONAL MECHANISMS OF INTERACTION BETWEEN NATIONAL SECURITY AND PRIORITY INTERESTS OF CIVIL SOCIETY

ІНСТИТУЦІЙНІ МЕХАНІЗМИ ВЗАЄМОДІЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ПРІОРИТЕТНИХ ІНТЕРЕСІВ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

The article is devoted to the analysis of the role of state national policy within the system of ensuring Ukraine's national security. The paper examines the primary directions of state national policy, its goals, and objectives, and identifies the connection between the effectiveness of national policy and the level of national security. Particular attention is paid to the analysis of problems and challenges Ukraine faces in the sphere of national security, as well as the role of state national policy in overcoming them. It is argued that in the modern world, state national policy plays a key role in ensuring the stability and security of the country. The development and implementation of an effective national policy is not only a task of public administration but also a crucial factor in ensuring national security.

It is shown that there is support from the population regarding the interaction between the state and civil society; this interconnectedness allows society to develop a system of non-governmental public institutions, determining the level of interaction between national security and state interests. The article characterizes the system of views on ensuring the security of the individual, society, and the state in Ukraine against external and internal threats in all

spheres of life. It is demonstrated that the fulfillment of national interests, in the context of their interconnection with national security, is determined not only by the protection of the economy but also by other vital spheres of modern society.

Keywords: *state national policy; national security; security of the country; public administration; stability of the country.*

Стаття присвячена аналізу ролі державної національної політики у системі забезпечення національної безпеки України. Аналізуються основні напрямки державної національної політики, її цілі та завдання, а також виявляє зв'язок між ефективністю національної політики та рівнем національної безпеки, причому, особлива увага приділяється аналізу проблем та викликів, з якими стикається Україна у сфері національної безпеки, та ролі державної національної політики у їхньому подоланні. Стверджується, що у сучасному світі державна національна політика відіграє ключову роль у забезпеченні стабільності та безпеки країни. Розробка та реалізація ефективної національної політики є не лише завданням державного управління, а й найважливішим фактором забезпечення національної безпеки.

Показано, що з боку населення йде підтримка щодо взаємодії держави та громадянського суспільства, цей взаємозв'язок дозволяє соціуму розвивати систему недержавних громадських інститутів, визначаючи рівень взаємодії національної безпеки та інтересів держави. Охарактеризовано систему поглядів на забезпечення в Україні безпеки особистості, суспільства та держави від зовнішніх та внутрішніх загроз у всіх сферах життєдіяльності. Показано, що забезпечення національних інтересів у ракурсі взаємозв'язку з національною безпекою визначається не лише захистом економіки, а й в інших сферах життєдіяльності сучасного суспільства.

Ключові слова: *державна національна політика, національна безпека, безпека країн,; публічне управління, стабільність країни.*

Problem Statement. Under the current conditions of global transformations and the ongoing military aggression against Ukraine, the issue

of national security extends beyond the purely military defense of territories. The relevance of this problem is driven by the need to rethink the role of state national policy as the foundation of social stability. There is an urgent need to analyze how the interaction between state institutions and civil society affects the protection of national interests. The problem lies in finding an optimal mechanism for harmonizing the interests of the individual, society, and the state, as well as overcoming new challenges (such as separatism, xenophobia, and migration crises) that threaten the country's integrity and its sustainable development.

Analysis of Recent Research and Publications. The following scholars have researched this subject matter: Ya. Halych, O. Hordiichuk, Yu. Hrytsenko, S. Drobotov, V. Melnyk, V. Naida, Yu. Shevchuk, Yu. Shemshuchenko, and others. The works of the aforementioned scientists confirm that the role of civil society in ensuring Ukraine's national security is of a transformational, critical, and multifunctional nature. Researchers note an evolution from the traditional function of oversight to active participation in ensuring the state's national security amidst the Russo-Ukrainian war.

Formulation of the Objective. The purpose of this article is to conduct a comprehensive analysis of the role of state national policy within the system of ensuring Ukraine's national security, to investigate the interconnection between the interests of civil society and state stability mechanisms, and to substantiate priority areas for interaction between the state and society to counter modern external and internal threats.

Main body of the paper. An important aspect of ensuring Ukraine's national security is the implementation of a state national policy focused on creating conditions for the harmonious coexistence and development of all peoples inhabiting the country. In this context, the development and implementation of the conceptual foundations of state national policy, reflecting modern requirements and challenges and aimed at strengthening the state, acquire particular significance.

According to M.N. Ruban, the core principles of the concept of Ukraine's state national policy are based on respect for human and civil rights and freedoms, regardless of national affiliation, and the provision of equal

e-ISSN 2786-5533

opportunities for the cultural, socio-economic, and spiritual development of all ethnicities and national groups. The policy is aimed at maintaining peace and harmony in a multi-ethnic society, preventing conflicts on national grounds, and protecting the interests of the Ukrainian diaspora abroad. An important component is state development and increasing the role of regions in the implementation of national policy, which contributes to strengthening state unity and territorial integrity.

Ukraine's state national policy also implies active involvement of citizens in the process of state governance, promoting the formation of civil society, and strengthening social solidarity. The introduction and effective implementation of these conceptual guidelines allow for the creation of conditions for the stable development of Ukraine, the strengthening of its sovereignty and national security, which, in turn, contributes to improving the quality of life and ensuring social protection against the backdrop of global and internal challenges.

One of the key tasks of a state striving for sustainable development and the preservation of its sovereignty is the provision of national security; this issue acquires special urgency. National security here acts not only as a means of military defense but also as a guarantee of the stability of socio-political life, economic development, and the preservation of cultural and national diversity [3, p. 27].

At the center of state national policy aimed at ensuring national security lies the concept of a balanced consideration of the interests of all national groups living in Ukraine. This implies creating conditions for their harmonious coexistence and development, preventing inter-ethnic conflicts and extremism. The fundamental principles here are the equality of all citizens before the law and the guarantee of human and civil rights and freedoms, regardless of national affiliation.

Effective national security is impossible without a stable internal political course that supports social unity and inter-ethnic harmony. An equally important aspect is an active foreign policy aimed at protecting the rights and interests of compatriots abroad, which also contributes to strengthening Ukraine's foreign policy position and its image on the international stage.

e-ISSN 2786-5533

Thus, an interim conclusion can be drawn that the conceptual foundations of Ukraine's national security are closely linked to the state national policy, which serves as a vital tool for achieving social stability, economic prosperity, and maintaining peace and harmony in a multi-ethnic society.

We agree with the opinion of G.M. Karpenko and N.O. Denisov that Ukraine's state national policy, aimed at supporting and developing a multi-ethnic society, makes a significant contribution to ensuring the stability and national security of the country in its unique ethnic and cultural diversity, which requires a carefully constructed approach to managing national relations [4].

One of the key aspects of the political and legal provision of security in multi-ethnic Ukraine is the improvement of legislation in the sphere of national relations. This involves creating a regulatory framework that prevents inter-ethnic conflicts and promotes the integration of all nations and ethnicities into a single social space. A key role here is played by the constitutional consolidation of equality and the protection of human rights and freedoms regardless of national affiliation.

Another important direction is the development and support of cultural dialogue between various ethnic and religious groups: state support for cultural diversity contributes to the strengthening of inter-ethnic and intercultural harmony.

Special attention is paid to developing measures for integrating representatives of all nations into the socio-economic process of the country. This includes providing equal opportunities in employment, education, and access to social infrastructure. Such measures allow for the elimination of the economic and social isolation of ethnic minorities, stimulating their active participation in the life of society [10, p.251].

Furthermore, a comprehensive approach to the political and legal provision of Ukraine's national security—including legal protection of citizens and support for cultural diversity—creates a stable foundation for the development of a harmonious and supportive society capable of withstanding challenges to its security and stability.

At the present stage, the main tasks of Ukraine's state national policy are the prevention of conflicts and the development of intercultural and inter-religious dialogue. Implementing these tasks requires a competent approach and attentive attitude toward citizens, as well as the development of measures that reduce social tension and strengthen civil peace and harmony.

Great importance within the framework of ensuring Ukraine's national security is attached to projects and initiatives aimed at strengthening a culture of peace, tolerance, and mutual understanding between different ethnic communities. This contributes to the formation of a cohesive society, which ultimately serves as a reliable basis for the stability and prosperity of the state on the international stage.

It must be emphasized that Ukraine's state national policy at the current stage plays a key role in ensuring national security, prioritizing the strengthening of inter-ethnic harmony and the maintenance of social stability in the country.

In modern Ukrainian reality, national security issues are inextricably linked with the effectiveness of state national policy. According to B.M. Bykova, "one of the key aspects of this policy is countering manifestations of nationalism, ethno-national separatism, and the threat of terrorism, which represent not only a challenge to the country's internal stability but also a critical point at which the state's ability to ensure the protection of its citizens and territorial integrity is determined" [7, p. 159].

To ensure national security, it is necessary to adopt a number of measures aimed at reducing tension and preventing possible conflicts:

1. Cultivating a sense of patriotism and civic identity among Ukrainian citizens, prioritizing the interests of the state above all;
2. Integrating migrants through educational programs, the study of the Ukrainian language and culture, and an understanding of rights and duties—all of which must become a mandatory part of national policy;
3. Active counteraction to manifestations of xenophobia and extremism, facilitated by both legislative initiatives and the work of public organizations.

e-ISSN 2786-5533

Migration processes play a critical role in ensuring the national security of any state, including Ukraine. Migration can contribute to economic growth and cultural enrichment; however, it can also become a source of social, economic, and political tension, especially if the level of migrant integration into society is insufficient.

Before analyzing the organization of interaction and the connection between national security and national interests, let us explain the primary matrix for typifying legally significant behavior, its legal attitudes and values, unique legal understanding, system of meaning-making, legal experience, and legal thinking. Adjusting the assessment of the institution of interaction in the socio-cultural space, we note that the implementation of the legal activity of the mechanism for organizing the protection of national interests and the large-scale consideration of social relations allows for the formation of specific directions of national strategic policy. In this case, the priority is the inviolability of human and civil rights and freedoms, society, and the state [5, p.24].

In this context, the professional activity of organizations and civil society institutions is also considered, especially the consolidation of the population and law enforcement, administrative, state, and municipal bodies—including their state apparatus and political organizations—while continuing to form a state-legal mentality. As the practice of the Ukrainian construct of the country's social system shows, when identifying problems of societal instability, it is necessary to reflect the specifics of national interests, both state and regional. This explanation in the interpretation of strategic concepts of state policy proves the basic condition for organizing the interconnection of interests and their security, enabling Ukraine to serve as a demonstrative example for the states of the world in the field of a true struggle for the national interests of society. Simultaneously, one should not forget about strengthening the country's role in ensuring internal stability and increasing the economic, political, and spiritual potential of society.

In all directions, the organization of interaction forms a legal mechanism for implementing national interests. Taking into account the interpretation of the interconnection between national security and the interests of society, the main functions of the organizational activity of society's legal institutions—

which influence the formation of social attitudes and form the vital organism of social consolidation—should be highlighted. These include significant basic human needs, usually in the socio-economic and spiritual spheres, which determine social relations and functions responsible for fulfilling core tasks; they implement a unified state policy, marked by constitutional provisions and norms of Ukrainian legislation, and form the foundations for interaction between state authorities and the people. At the same time, the internal and external potential of Ukraine's national security strategy should be considered, putting forward provisions of military policy and the tasks of military-economic provision for the country's defense [6].

The evidence of such national unity, the spiritual traditions of the people, and the level of statehood development reflect the concept of ensuring interests, while also considering the "individual, society, and state" context. In this case, it assumes the recognition of the rights of the interacting parties—state, society, and individual—with the legal institutions of civil society standing at the head of this system. Today, in theory and practice, the most frequently used interpretations of "national interests" and "national security" are politicized and used in almost all spheres of life [1, p.22].

At the same time, national interests at the state, regional, and global levels are formulated by specific subjects, building a security system within the framework of legal regulation of state authorities and society. At the head of such a system is a complex, multifaceted process of preventing threats to the state. Evaluating the system of protecting national interests, let us turn to their specific features and, through a legal prism, reveal their legislative constructs forming in the socio-economic and spiritual-moral mechanism of society's development.

One such direction is the strengthening of the country's economic sovereignty and ensuring economic sustainability at the domestic and international levels. In this regard, the stability of the financial system is also necessary. The modern interconnection of foreign economic cooperation and the implementation of competitiveness in the economic sector create an element of protection for national interests, taking into account human potential. Since the adoption of strategic tasks, issues of economic security

have been repeatedly considered at interdepartmental meetings of the Security Council of Ukraine, where the main problems of strategic planning were noted and the importance of risk measures for socio-economic development was analyzed; alongside this, adjustments for predicting and preventing economic threats were adopted [2].

Forecasting the provision of economic security is formed in two blocks of the protection mechanism: the so-called defense against the impact of negative threat factors and the "offense" in the form of implementing economic interests. As we can see, counteracting economic threats is linked to protection and preventing danger within the Ukrainian economy. Furthermore, in the economic space, economic protection is implemented through other legal documents. Civil legislation defines the legal status of participants in civil turnover, while the laws of Ukraine define the legal foundations of the mechanism for ensuring the unity of the economic space. The functions of the criminal-legal provision of the economic security of organizations against crimes in the sphere of economic activity are prescribed in the Criminal Code of Ukraine.

A significant step toward strengthening national security is the adaptation of national policy to modern global realities, which requires the state to be flexible and capable of reacting quickly to the changing international situation and promoting the development of civil society.

We believe it is necessary to pay attention to the development of regional programs aimed at: the economic and cultural revitalization of national regions, which can serve as an additional incentive for strengthening the country's unity and preventing separatist sentiments; investments in educational programs, including the study of the history and culture of Ukraine, will also become an important aspect of supporting national identity and patriotism. Improving state national policy is seen as a multifaceted area of work that not only strengthens national security but also contributes to the creation of a more harmonious, robust, and unified Ukrainian society.

e-ISSN 2786-5533

References:

1. Antoshkin, V. K. (2014). Sutnist sotsialno-ekonomichnoi bezpeky rehioniv ta yii zviazok z natsionalnoiu bezpekoiu derzhavy [The essence of socio-economic security of regions and its connection with the national security of the state]. Visnyk Berdianskoho universytetu menedzhmentu i biznesu, (3), 17–23.

2. Hlubochenko, K. O. (2011), "Functioning of mechanisms of interaction between state authorities and the public in the state administration system", Derzhavne budivnytstvo, № 2, retrieved from : http://nbuv.gov.ua/j-pdf/DeBu_2011_2_7.pdf.

3. Zhovnirchyk, Ya. F. (2013), "Directions for optimizing relations between public authorities and institutions of civil society", Naukovyi visnyk Akademii munitsypalnoho upravlinnia. Seriia : Upravlinnia, vol. 4, pp. 25–32, retrieved from : http://nbuv.gov.ua/jpdf/Nvamu_upravl_2013_4_5.pdf.

4. Melnyk, L. A. (2019), "Interaction of the state and institutions of civil society: basic concepts, problems and strategic directions", Derzhavne upravlinnia: udoskonalennia ta rozvytok, №2, retrieved from: http://www.dy.nayka.com.ua/pdf/2_2019/30.pdf.

5. Podolska, Ye. A., & Nazarkin, P. O. (2015). Novyi sens y innovatsiini sposoby zabezpechennia sotsialnoi bezpeky [New meaning and innovative ways to ensure social security]. Visnyk Odeskoho natsionalnoho universytetu. Seriia: Sotsiolohiia i politychni nauky, 20(2), 19–25.

6. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018 No. 2469-VIII [On National Security of Ukraine: Law of Ukraine dated 21.06.2018 No. 2469-VIII]. Available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text

7. Sydorchuk, O. H., & Khandii, O. O. (2019). Instytutsiine zabezpechennia derzhavnoho rehuliuvannia sotsialnoi bezpeky [Institutional support for state regulation of social security]. Ekonomichnyi visnyk Donbasu, (1), 157–163.

8. Sychenko, O. O. (2012). Sotsialna bezpeka v systemi natsionalnoi bezpeky derzhavy [Social security in the system of national security of the state]. Naukovi pratsi Chornomorskoho derzhavnoho universytetu imeni Petra

Mohyly kompleksu «Kyievo-Mohylianska akademiia». Ser.: Derzhavne upravlinnia, 186(174), 34–38.

9. Stratehiia natsionalnoi bezpeky Ukrainy: RNBO; Rishennia vid 14.09.2020, zatv. Ukazom Prezydenta Ukrainy vid 14.09.2020 r. No. 392/2020 [National Security Strategy of Ukraine: NSDC; Decision of 14.09.2020, approved by the Decree of the President of Ukraine of 14.09.2020 No. 392/2020]. Available at: https://zakon.rada.gov.ua/laws/show/n0005525-20#Text

10. Shakhmatova, T. A. (2014). Tendentsii formuvannia ta rozvytku systemy zabezpechennia sotsialnoi bezpeky natsionalnoi ekonomiky [Trends in the formation and development of the system for ensuring social security of the national economy]. Universytetski naukovi zapysky, (4), 249–256.

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: 02.05.26
Accepted: 28.05.26
Published: 26.06.26

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.

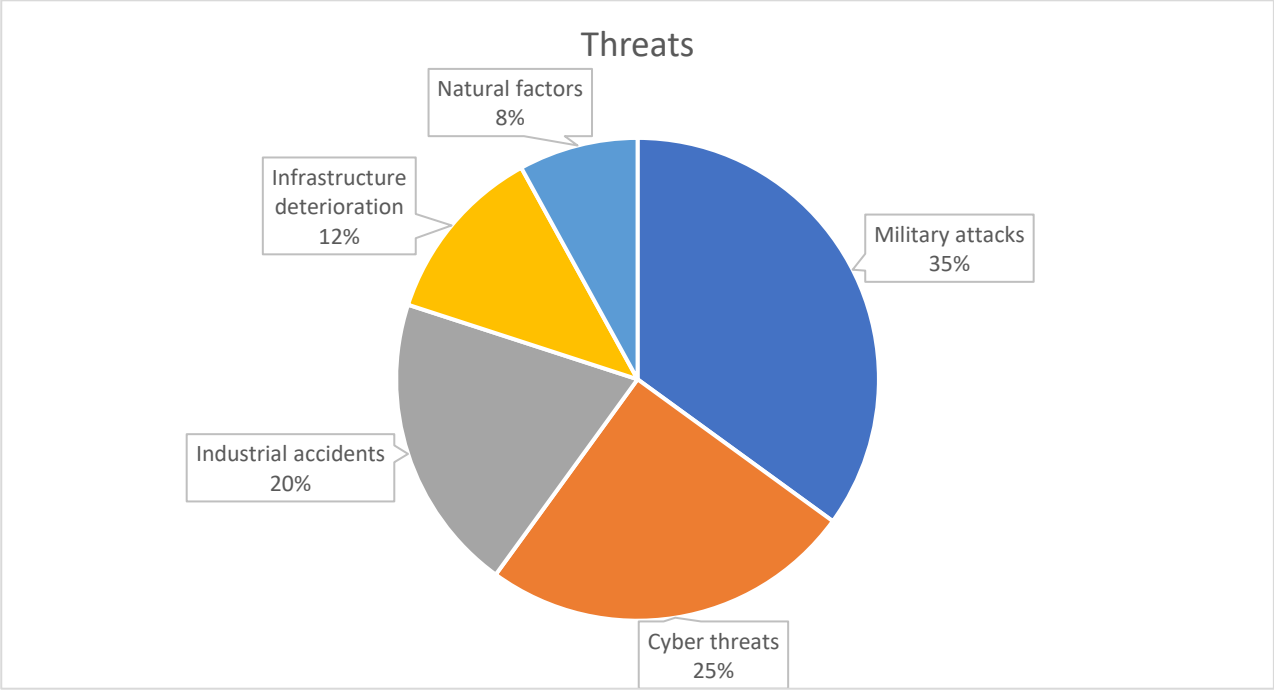

Figure 1. Analytical and Expert-Based Structure of Key Threats to Critical Energy Infrastructure in the International Context

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.

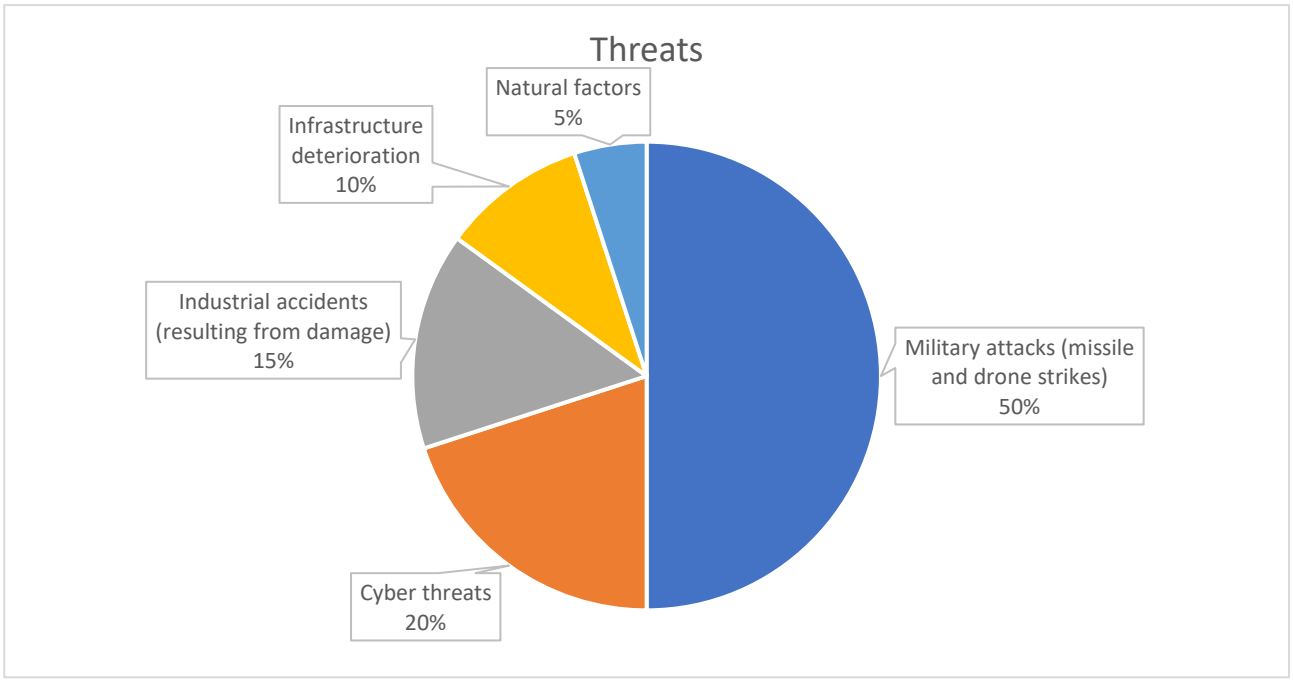

Figure 2. Analytical and Expert-Based Structure of Key Threats to Critical Energy Infrastructure in Ukraine under Current Conditions

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

DOI: 10.52363/passa-2026.1-27
UDC: 351 (477): 322

Siemilietov O., *Senior Researcher at the Research Laboratory of Civil Security Management of the Educational and Research Institute of Civil Defense, National University of Civil Defense of Ukraine, Cherkasy*
ORCID: 0000-0002-7903-0098

Berezynskyi L., *Associate Professor of the Department of Educational Management, State Policy and Economics, Communal Institution of Higher Education "Dnipro Academy of Continuing Education" of Dnipropetrovsk Regional Council*
ORCID: 0009-0003-3387-4601

Сємілєтов О., *старший науковий співробітник науково-дослідної лабораторії з дослідження проблем управління у сфері цивільного захисту Навчально-наукового інституту цивільного захисту Національного Університету Цивільного Захисту України, Черкаси*

Березинський Л.В., *докторант, Комунальний заклад вищої освіти «Дніпровська академія неперервної освіти»*

APPLYING THE EXPERIENCE OF EU COUNTRIES IN SHAPING SECURITY POLICY IN UKRAINE

ЗАСТОСУВАННЯ ДОСВІДУ КРАЇН ЄС У ФОРМУВАННІ ПОЛІТИКИ БЕЗПЕКИ В УКРАЇНІ

This study examines the transformation of Ukraine's national security system in the context of ongoing armed aggression and the need to implement Euro-Atlantic standards. The relevance of this work stems from the need to adapt national legislation to the requirements of the Association Agreement with the

EU and the experience of NATO countries, which necessitates a review of existing regulatory acts and the introduction of modern management mechanisms. The evolution of the armed conflict since 2014 is analyzed as a consequence of the Russian Federation's violation of fundamental international agreements (the UN Charter, the Helsinki Final Act). Particular attention is paid to the transition from hybrid warfare tactics to the full-scale invasion of 2022, which served as a catalyst for a paradigm shift in state governance: from a reactive model of "passive defense" to a proactive strategy of deterrence. It is argued that the modern security architecture must be based on the synergy of "hard" (military power) and "soft" (social cohesion, diplomacy) power. The author emphasizes that the implementation of civilian control over the security sector is a fundamental safeguard against corruption and the usurpation of power. It has been found that, in addition to military threats, the demographic crisis, mass migration, environmental damage, and the need to reintegrate veterans represent critical challenges to Ukraine's sustainable development. It is concluded that ensuring national security requires a comprehensive approach that combines the technological modernization of the Armed Forces with the creation of a favorable socio-economic climate for the preservation and return of human capital.

Keywords: *public administration, national security, Euro-Atlantic integration, hybrid warfare, regulatory adaptation, human capital, state resilience.*

У роботі досліджено трансформацію системи національної безпеки України в умовах триваючої збройної агресії та необхідності імплементації євроатлантичних стандартів. Актуальність роботи зумовлена потребою адаптації національного законодавства до вимог Угоди про асоціацію з ЄС та досвіду країн НАТО, що вимагає перегляду існуючих нормативно-правових актів та впровадження сучасних управлінських механізмів. Проаналізовано еволюцію збройного конфлікту, починаючи з 2014 року, як наслідок порушення російською федерацією фундаментальних міжнародних угод (Статуту ООН, Гельсінського заключного акта). Особливу увагу приділено переходу від тактик гібридної війни до повномасштабного вторгнення 2022 року, що стало

каталізатором для зміни парадигми державного управління: від реактивної моделі «пасивного захисту» до проактивної стратегії стримування. Обґрунтовано, що сучасна архітектура безпеки має базуватися на синергії «жорсткої» (військова потужність) та «м'якої» (соціальна згуртованість, дипломатія) сили. Автор наголошує, що впровадження цивільного контролю над сектором безпеки є фундаментальним запобіжником проти корупції та узурпації влади. Виявлено, що окрім воєнних загроз, критичними викликами для сталого розвитку України є демографічна криза, масова міграція, екологічні збитки та необхідність реінтеграції ветеранів. Зроблено висновок, що забезпечення національної безпеки потребує комплексного підходу, який поєднує технологічну модернізацію Збройних Сил із формуванням сприятливого соціально-економічного клімату для збереження та повернення людського капіталу.

Ключові слова: *публічне управління, національна безпека, євроатлантична інтеграція, гібридна війна, нормативно-правова адаптація, людський капітал, стійкість держави.*

Problem statement. In order to bring national legislation into line with the requirements of regulatory acts specifically, in accordance with the Association Agreement on Ukraine's accession to the EU and the implementation of best practices from EU and NATO countries-there is a pressing need to analyze and take steps to amend Ukraine's regulatory acts.

Thus, today, in an era of rapid technological development and global changes in the world, issues regarding the adaptation of legislation are highly relevant. The goal of such adaptation is to incorporate modern best practices and develop new approaches to implementing governance mechanisms specifically, addressing the contemporary challenges that arise during the active development of the state across all spheres of life, as well as when formulating plans for its further development in economic and political activities and on the global stage.

That is, the start of the armed aggression in 2014, which occurred due to violations of treaties, agreements, and obligations on the part of the leadership

of the Russian Federation specifically, violations of the following legal documents governing the fundamental relations between the successor states: "On the Establishment of the Commonwealth of Independent States" dated December 8, 1991[2], the Charter of the United Nations [15], and the Final Act of the Conference on Security and Cooperation in Europe (Helsinki Final Act) [3] by violating territorial integrity, specifically by employing elements and tactics of information and hybrid warfare: interference in a state's internal politics through the use of new methods of waging geopolitical wars and achieving political objectives.

It should be noted that, despite the use of hybrid warfare tactics between Ukraine and the Russian Federation, the effectiveness of achieving objectives has been limited, as our country has adopted a policy of deterrence and passive defense, utilizing conflict resolution mechanisms and seeking international support. It should be noted that the aggressive, expansionist policy of the Russian Federation's leadership led to the next stage of deterioration in relations between the two states, which escalated into full-scale hostilities initiated by the Russian Federation on the morning of February 24, 2022, along the entire length of Ukraine's state border, following the violation of the state border by the Russian Federation's armed forces and the prior delivery of strategic and ballistic strikes against critical and military infrastructure.

It should be noted that the issue of national security-following the annexation of the Autonomous Republic of Crimea and parts of the Donetsk and Luhansk regions in 2014, and the deterioration of relations with the Russian Federation due to the annexation of part of Ukraine's territory is highly relevant but, in light of external and internal threats, requires updating and further scientific research.

Analysis of recent research and publications Issues of national security are the focus of attention for a wide range of scholars. In particular, the general aspects of this topic have been studied by a group of authors, including V. Bakumenko, A. Degtyar, I. The theoretical and methodological foundation for research in this field was laid by the works of scholars such as V. Bachinin, V. Vovk, O. Hryshchuk, O. Danilyan, A. Kozlovsky, and others. At the same time, S. Abakumov, O. Belkov, V. Gorbulin, V. Lipkan, H. Sytnik, L. Chekalenko. Drawing

on this extensive body of theoretical work has made it possible to thoroughly examine the essence of a state's national security in the context of building a civil society.

Presentation of the main material: An investigation into the contemporary challenges and threats facing Ukraine requires a retrospective analysis of the evolution of the domestic national security sphere, which began its conceptual formation in the early 20th century and acquired a qualitatively new meaning after the country gained state sovereignty in 1991. Changes in the geopolitical environment, globalization processes, and the gradual decline in the influence of international security institutions established in the post-war period for the peaceful resolution of conflicts actualize the objective need to rethink and modernize security doctrines. The fundamental principles of the state's national security are enshrined in the Constitution of Ukraine [16]. Specifically, Article 18 defines the provision of national security as one of the key guidelines of the state's foreign policy, while Article 34 establishes the legitimate possibility of restricting the exercise of citizens' constitutional rights in the interests of national security. Furthermore, Article 92 stipulates that the foundations of national security are determined exclusively by the laws of Ukraine.

The Basic Law also establishes a clear institutional distribution: the President of Ukraine acts as the guarantor of state sovereignty and security; the National Security and Defense Council serves as the coordinating body; and the Cabinet of Ministers is responsible for the practical implementation of relevant measures. Certain constitutional articles determine specific components of security without explicitly classifying them as elements of national security; for instance, Article 16 establishes the state's duty to ensure environmental security, while Article 17 declares the protection of economic and information security, as well as the defense of the state border, to be the most important functions of the state [16].

State policy in the field of security is implemented through a hierarchical system of strategic and regulatory acts, where the Law of Ukraine "On National Security"[18] serves as the basic architectural element, further detailed through the National Security Strategy, the Military Security Strategy, the Strategy for the Development of the Defense-Industrial Complex, and the Cybersecurity

e-ISSN 2786-5533

Strategy. An analysis of the security concepts of allied countries demonstrates a comprehensive approach to identifying global threats. For instance, Japan's 2013 National Security Strategy identifies key challenges such as shifts in the balance of power, rapid technological development, the proliferation of weapons of mass destruction, international terrorism, threats to global resources, and challenges to human development [11]. Similarly, the 2022 US National Security Strategy defines the current decade as decisive for formalizing the terms of geopolitical competition among major powers, emphasizing the imperative of adhering to the principles of self-determination, territorial integrity, and political independence, as well as the need to strengthen international institutions, protect human rights, and ensure equal conditions and opportunities within the global economy [13]. Ukraine's national security is currently challenged by a complex matrix of external and internal threats. Externally, the state confronts direct military aggression aimed at territorial occupation, state-sponsored terrorism, the systematic destruction of energy and economic infrastructure, information and cyber warfare, and the latent influence of hostile organized crime.

These specific threats are further amplified by the modern paradigm of globalization, which facilitates transnational crimes such as illicit trafficking, ideological extremism, and the proliferation of weapons of mass destruction. Concurrently, domestic vulnerabilities persist, necessitating continuous efforts to eradicate systemic corruption, abuse of office, and information manipulation through advanced digital oversight mechanisms, including electronic declarations and transparent public procurement systems. In response to these multidimensional challenges, the state's primary strategic objectives encompass repelling the armed aggression to restore the 1991 territorial borders, securing critical infrastructure, and mitigating the socio-economic consequences of the war. This involves driving infrastructural and economic recovery, facilitating the reintegration of veterans and displaced persons, addressing acute demographic and environmental crises, and mobilizing international assistance.

These national imperatives unfold within a highly volatile geopolitical environment characterized by a shifting balance of power and intense strategic

competition on the Eurasian continent among major centers of influence namely the EU, the United States, China, and a revanchist Russia seeking to restore its Soviet-era dominance. Within this complex geopolitical reality, the modern national security architecture must fundamentally transcend outdated historical frameworks such as the 2003 Law "On the Fundamentals of National Security," which marginalized the role of citizens by clearly defining and fully integrating civil society into the state's comprehensive defense and security apparatus [12].

Ukraine’s national security framework, anchored by the 2021 National Security Strategy and the Law "On National Security," mandates a defense posture based on deterrence, resilience, and Euro-Atlantic integration. However, the legal architecture exhibits notable gaps, such as limited mechanisms for direct citizen oversight and incomplete regulatory implementation for critical infrastructure protection. The full-scale Russian invasion necessitated a radical recalibration of these priorities, elevating immediate combat readiness, the rapid modernization of the Armed Forces, and the accelerated expansion of domestic defense production to the forefront of state policy.

This conflict has simultaneously underscored the changing nature of modern warfare, revealing that even allied nations would struggle to repel a fully mobilized, experienced adversary without fundamental tactical adaptations. Consequently, Ukraine's strategic transition involves not only battlefield innovation but also the rigorous implementation of democratic oversight models such as parliamentary control over intelligence and the functional separation of law enforcement and security agencies, mirroring established practices in the United States, the United Kingdom, and Germany. While centralized wartime command ensures operational efficiency, it must be balanced with transparency and supranational monitoring to safeguard democratic values and prevent institutional overreach. Domestically, this security transformation is complicated by acute socio-military challenges, including the psychological exhaustion of mobilized personnel, the lack of viable rotation and demobilization protocols, and the urgent imperative to confiscate illegal firearms from the civilian population. Furthermore, the war

has catalyzed a severe demographic crisis driven by mass youth emigration rooted in economic instability, acute security threats, and systemic governance issues. Addressing these compounding vulnerabilities requires the state to synergize "hard" military defense with "soft" post-war recovery strategies including robust international reconstruction funding, economic incentivization, and systemic institutional reforms to restore public trust, ensure sustainable development, and secure long-term national resilience.

Conclusions: An analysis of the security policy-making process in Ukraine through the lens of the experience of EU countries and Euro-Atlantic partners suggests that, in the current environment, national security has moved beyond the confines of a purely military doctrine. The Russian Federation's armed aggression against Ukraine has become a catalyst for irreversible transformations that require a shift from a reactive governance model to a proactive strategy of deterrence and resilience. It has been demonstrated that an effective security architecture must be based on the synergy of "hard" (military power, defense industry) and "soft" (social cohesion, economic development, diplomacy) instruments. The integration of European standards and democratic and civilian oversight of the security sector is not only a requirement of international partners but also a fundamental safeguard against the usurpation of power and corruption.

It has been found that, in addition to external military threats, critical challenges for Ukraine's future include the demographic crisis, youth migration, a high crime rate, the economic crisis, the critical vulnerability of the state's territory, significant damage to the environment and architectural heritage, and the need to integrate veterans. Thus, ensuring national security for future generations requires a comprehensive approach: from the technological modernization of the armed forces to the creation of a favorable socio-economic climate capable of retaining human capital and ensuring the sustainable development of a democratic state.

References:

1. Administration of the State Service for Special Communications and Information Protection of Ukraine. (2023, February 6). On the approval of the

procedure for routing calls during emergency communications via the single emergency number 112 in the public electronic communications network (Order No. 89). Legislation of Ukraine. https://zakon.rada.gov.ua/go/z0493-23

2. Commonwealth of Independent States. (1991, December 8). Agreement on the establishment of the Commonwealth of Independent States. Legislation of Ukraine. https://zakon.rada.gov.ua/go/997_077

3. Conference on Security and Cooperation in Europe. (1975, August 1). Final act of the Conference on Security and Cooperation in Europe (Helsinki Final Act). Ukrainian Legislation. https://zakon.rada.gov.ua/go/994_055

4. European External Action Service. (2016, June). Shared vision, common action: A stronger Europe. A global strategy for the European Union's foreign and security policy. https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

5. Ministry of Youth and Sports of Ukraine. (2026). The situation of youth in Ukraine: "Youth of Ukraine: Challenges and adaptation under martial law": Annual report to the President of Ukraine, the Verkhovna Rada of Ukraine, and the Cabinet of Ministers of Ukraine on the situation of youth in Ukraine (based on the results of 2022–2025). https://mms.gov.ua/storage/app/sites/16/Molodizhna_polityka/2026/2025-shhoricna-dopovid-pu-vru-kmu-molod-ukrayini.pdf

6. National Institute for Strategic Studies. (2013). On the priority tasks of Ukraine's foreign policy: An analytical report. https://niss.gov.ua/sites/default/files/2013-12/0312_dopovid.pdf

7. NATO. (2021, June 14). Brussels summit communiqué. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/brussels-summit-communique

8. Pashieva, A. (2023). The creation of a secure environment as a key driver of Ukraine's development. The security situation in Ukraine in the context of war: Current state, threats, and directions for security, 20–21. https://www.knuba.edu.ua/wp-content/uploads/2023/11/zbirnyk_kruglyj-stil_26.09.2023.pdf

9. President of Ukraine. (2021, March 25). On the decision of the National Security and Defense Council of Ukraine dated March 25, 2021, "On the military security strategy of Ukraine" (Decree No. 121/2021). Legislation of Ukraine. https://zakon.rada.gov.ua/go/121/2021

10. Prime Minister's Office. (2015, November). National security strategy and strategic defence and security review 2015: A secure and prosperous United Kingdom. https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

11. Prime Minister's Office of Japan. (2013, December 17). National security strategy. https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf

12. Reznikova, O. O. (2022). National resilience in a changing security environment. NISD. https://doi.org/10.53679/NISS-book.2022.01

13. The White House. (2022, October). National security strategy. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

14. The White House. (2025, December). National security strategy of the United States of America. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

15. United Nations. (1945, June 26). Charter of the United Nations (as amended). Statute of the International Court of Justice of the United Nations. Legislation of Ukraine. https://zakon.rada.gov.ua/go/995_010

16. Verkhovna Rada of Ukraine. (1996, June 28). Constitution of Ukraine (No. 254k/96-VR). Legislation of Ukraine. https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80

17. Verkhovna Rada of Ukraine. (2012, March 13). On the emergency assistance system for the public via the single telephone number 112 (Law No. 4499-VI). Legislation of Ukraine. https://zakon.rada.gov.ua/go/4499-17

18. Verkhovna Rada of Ukraine. (2018, June 21). On the national security of Ukraine (Law No. 2469-VIII). Legislation of Ukraine. https://zakon.rada.gov.ua/go/2469-19

19. Verkhovna Rada of Ukraine. (2021, November 16). On critical infrastructure (Law No. 1882-IX). Legislation of Ukraine. https://zakon.rada.gov.ua/go/1882-20

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: 27.03.26
Accepted: 27.05.26
Published: 26.06.26

DOI: 10.52363/passa-2026.1-28
UDC: 351+005.52:005.334

Tverdokhlib O., *Doctor of Science in Public Administration, Professor, Leading researcher at Regulatory Research Department, Institute of Research in Civil Protection, National University of Civil Protection of Ukraine, Kyiv*
ORCID: 0000-0002-1502-2937

Teslenko O., *PhD in Governance and Public Administration Deputy Head at Regulatory Research Department, Institute of Research in Civil Protection, National University of Civil Protection of Ukraine, Kyiv*
ORCID: 0000-0002-1003-8876

Shtyka B., *lecturer at the department of advanced training and specialized preparation in the field of civil protection, Educational and Scientific Institute of Engineering and Specialized Training, National University of Civil Protection of Ukraine, Cherkasy*
ORCID: 0009-0002-4343-4928

Твердохліб О., *доктор наук з державного управління, професор, провідний науковий співробітник науково-дослідного відділу нормативного регулювання науково-дослідного центру нормативно-технічного регулювання, Інститут наукових досліджень з цивільного захисту Національного університету цивільного захисту України, м. Київ*

Тесленко О., *доктор філософії, заступник начальника науково-дослідного відділу нормативного регулювання науково-дослідного центру нормативно-технічного регулювання, Інститут наукових досліджень з цивільного захисту Національного університету цивільного захисту України, м. Київ*

Штика Б., *викладач кафедри підвищення кваліфікації та спеціалізованої підготовки у сфері цивільного захисту, Навчально-науковий інститут*

інженерної та спеціальної підготовки Національного університету цивільного захисту України, м. Черкаси

RISK-ORIENTED GOVERNANCE IN CONTEMPORARY PUBLIC ADMINISTRATION: A COMPREHENSIVE THEORETICAL, METHODOLOGICAL, AND INSTITUTIONAL ANALYSIS

РИЗИКООРІЄНТОВАНИЙ ПІДХІД ДО ОРГАНІЗАЦІЇ УПРАВЛІННЯ В СУЧАСНОМУ ПУБЛІЧНОМУ УПРАВЛІННІ: КОМПЛЕКСНИЙ ТЕОРЕТИЧНИЙ, МЕТОДОЛОГІЧНИЙ ТА ІНСТИТУЦІЙНИЙ АНАЛІЗ

This research presents a comprehensive analysis of the transition toward risk-oriented governance in contemporary public administration, an evolution necessitated by the shift from post-war stability to systemic vulnerability. By reconceptualizing risk as a foundational category of governance rather than a technical variable, the study explores how modern institutions can enhance strategic capacity and reflexivity. A central pillar of this analysis is Ulrich Beck's "Risk Society" thesis, which posits a transition from the distribution of "goods" to the distribution of manufactured "bads", challenging the "organized irresponsibility" of traditional bureaucratic structures. The analysis incorporates the International Risk Governance Council (IRGC) framework, providing a multi-stakeholder pathway for managing systemic risks through interlinked phases of pre-assessment, appraisal, and evaluation.

Methodologically, the work advocates for pluralism, integrating quantitative data-driven models with qualitative expert insights to bridge the gap between objective indicators and subjective contexts. It also introduces "Evidential Pluralism" (EBP+) for robust policy evaluation. To address the 2024–2025 "polycrisis" landscape – characterized by compounding climate, geopolitical, and digital threats – the research utilizes the OECD's FIELD/SCOPES and the "AAA" (Antifragile, Anticipatory, Agility) frameworks to institutionalize proactivity. Economic flexibility is further addressed via Real Options Theory, treating public investments as dynamic options to manage uncertainty. Finally, the study warns against the "state of exception", where crisis-driven governance may normalize

e-ISSN 2786-5533

exceptional executive powers, and instead proposes an ethical framework built on ex ante accountability and integrated cross-sector resilience.

Keywords: *risk-oriented governance, public administration, polycrisis, systemic risk, institutional resilience, anticipatory governance, risk society, methodological pluralism.*

У цьому дослідженні представлено комплексний аналіз переходу до ризикоорієнтованої організації управління в сучасному публічному управлінні – еволюції, зумовленої переходом від післявоєнної стабільності до системної вразливості. Переосмислюючи ризик як фундаментальну категорію управління, а не як технічну змінну, у дослідженні розглядається, як сучасні інституції можуть підвищити свій стратегічний потенціал та рефлексивність. Цей аналіз базується на тезі Ульріха Бека про "суспільство ризику", яка передбачає перехід від розподілу "благ" до розподілу штучно створених "збитків", кидаючи виклик "організованій безвідповідальності" традиційних бюрократичних структур. Аналіз включає рамки, запропоновані Міжнародною радою з управління ризиками (IRGC), що забезпечують багатосторонній підхід до управління системними ризиками через взаємопов'язані етапи попередньої оцінки, аналізу та оцінювання.

З методологічної точки зору в цій роботі відстоюється принцип плюралізму, що передбачає поєднання кількісних моделей, заснованих на даних, з якісними експертними висновками з метою подолання розриву між об'єктивними показниками та суб'єктивним контекстом. Також у ній наведено концепцію "доказового плюралізму" (EBP+) з метою здійснення надійної оцінки відповідної політики. Для вирішення проблем "полікризи" 2024–2025 років, що характеризується поєднанням кліматичних, геополітичних та цифрових загроз, у дослідженні використано рамки FIELD/SCOPES та "AAA" (Antifragile, Anticipatory, Agility) OECP задля інституціоналізації проактивності. Гнучкість економіки також розглядається крізь теорію реальних опціонів, яка трактує державні інвестиції як динамічні опціони для управління невизначеністю. Окрім того, дослідження застерігає від "стану винятку", коли кризове

управління здатне нормалізувати надзвичайні виконавчі повноваження, і натомість пропонує етичну рамку, побудовану на попередній підзвітності та інтегрованій міжсекторальній стійкості.

Ключові слова: *ризикоорієнтований підхід до організації управління, публічне управління, полікриза, системний ризик, інституційна стійкість, проактивне управління, суспільство ризику, методологічний плюралізм.*

Problem statement. The administrative landscape of the twenty-first century is defined by a departure from the stability that characterized the post-war era. Contemporary public administration operates within governance environments that differ fundamentally from the bureaucratic structures envisioned by classical theorists. The prevailing conditions are marked by uncertainty, non-linearity, interdependence, and systemic vulnerability. These transformations are not merely peripheral; they challenge the foundational assumptions of traditional administrative models designed for hierarchical control and procedural certainty. Consequently, public administration must undergo a structural evolution to reconceptualize risk not as an external disturbance but as a foundational category of governance. This transition toward risk-oriented governance aims to enhance institutional reflexivity, strategic capacity, and long-term resilience.

Analysis of recent research and publications. Risk is a multidimensional construct that extends far beyond technical assessments of probability and impact. In the realm of public administration, risk functions as a lens through which uncertainty is interpreted, prioritized, and managed. It encompasses social perceptions, institutional responses, and normative judgments about public values. Risk propensity is not a stable characteristic of individuals or institutions but is deeply influenced by the socio-political context [11].

The most significant theoretical contribution to understanding this shift is the “Risk Society” thesis proposed by Ulrich Beck. Beck argues that modern society has transitioned from an industrial modernity, focused on the distribution of “goods” (wealth and resources), to a “second modernity” centered on the distribution of “bads” (risks and threats) [2]. These risks are

"manufactured" – they are unintended side effects of technological and economic progress [ibid.]. Unlike the natural disasters of the past, these hazards originate within the centers of rationality, science, and prosperity [ibid.].

Presentation of the main material. Classical bureaucratic models emphasized legal-rational authority, procedural certainty, and hierarchical coordination as the primary mechanisms for achieving administrative effectiveness. While these principles remain important, they are insufficient for addressing governance challenges characterized by rapid change, interdependence, and uncertainty. In such contexts, public administration must not only implement predefined rules but also anticipate, interpret, and manage risks that cannot be fully predicted or controlled.

Risk-oriented governance emerges as a response to these challenges. Rather than treating risk as an external disturbance or technical variable, this approach conceptualizes risk as an inherent feature of governance systems. From this perspective, governance is fundamentally concerned with making decisions under conditions of uncertainty and managing the consequences of those decisions for public values.

The risk society is characterized by "reflexive modernization", a phase where the side effects of industrialization can no longer be ignored by the existing institutional framework [7]. A critical feature of this era is "organized irresponsibility", where institutions intended to provide safety – the state, the scientific community, and the market – become the primary sources of unmanageable consequences [ibid.]. Because these risks often transcend human imagination and scientific determination, conventional standards of responsibility and monitoring fail [ibid.].

Conceptualizing risk as a structuring principle implies that risk considerations must permeate every stage of the policy cycle. In the past, risks were managed in a departmentalized manner – finance handled currency fluctuations, operations handled quality, and insurance handled liability [11]. Modern risk-oriented governance requires the integration of risk into the core of governance and compliance structures [ibid.]. This approach challenges silo-based structures, emphasizing the interconnected nature of policy domains.

e-ISSN 2786-5533

The trajectory of public administration theory has moved through three distinct archetypes: Public Administration (PA), New Public Management (NPM), and New Public Governance (NPG) [13]. Each paradigm reflects a different orientation toward the management of uncertainty and the role of the state (*Table 1*).

Traditional Public Administration (late 19th century to the late 1970s) focused on administrative procedures, legal-rational authority, and equality of treatment through hierarchy. However, as public needs outstripped resources, this model came under fire [ibid.]. The subsequent rise of New Public Management (NPM) in the late 1970s introduced private-sector techniques, emphasizing efficiency, "hands-on" management, and the organizational distancing of implementation from policy-making [ibid.]. While NPM improved operational performance, its intra-organizational focus limited its ability to address complex, cross-sectoral risks [ibid.].

New Public Governance (NPG) emerged at the start of the twenty-first century as a response to the limitations of NPM. NPG emphasizes pluralistic, communitarian, and participatory elements within a governance regime [ibid.]. It views policymaking and service delivery as collaborative processes within complex networks, prioritizing transparency, social justice, and interdependence [12]. This paradigm is particularly suited for risk-oriented governance because it acknowledges that modern "wicked problems" cannot be solved by the state alone; they require collaborative action and co-production with non-state actors [13].

Table 1. Features of Public Administration Paradigm

Paradigm	Governance Focus	Role of the State	Management Logic
Public Administration	Hierarchy & Law	Centralized Provider	Procedural Rule-Following
New Public Management	Efficiency & Markets	Purchaser/Regulator	Private-Sector Managerialism
New Public Governance	Networks & Pluralism	Facilitator/Partner	Collaboration & Co-production

Source: compiled by the author

To bridge the gap between technical risk assessment and democratic governance, the International Risk Governance Council (IRGC) developed an integrated analytic framework [15]. This framework provides guidance for the early identification and handling of risks characterized by complexity, uncertainty, and ambiguity [6].

The IRGC framework breaks down the risk process into four interlinked elements, supported by cross-cutting aspects such as communication and stakeholder engagement:

Pre-assessment: This stage involves identification and framing. It requires an early warning system and the involvement of relevant actors to capture diverse perspectives on the risk and its associated opportunities.

Appraisal: This consists of two parts: a technical risk assessment (evaluating impacts and severity) and a concern assessment (gathering knowledge about how people perceive the risk and its socio-cultural consequences).

Characterization and Evaluation: Decision-makers judge the significance and acceptability of the risk by comparing appraisal outcomes against specific criteria. This stage determines whether the risk is acceptable, tolerable, or intolerable.

Management: This involves designing and implementing actions to avoid, reduce, transfer, or take the risk. It requires managing trade-offs between risks and opportunities (Table 2).

Table 2. IRGC Framework

Framework Element	Key Components	Objective
Pre-assessment	Framing, Early Warning	Set boundaries and identify stakeholders
Risk Appraisal	Risk & Concern Assessment	Synthesize technical and social knowledge
Evaluation	Judgment of Acceptability	Determine need for management intervention
Risk Management	Implementation, Monitoring	Apply mitigation or adaptation strategies
Cross-cutting	Communication, Engagement	Ensure transparency and inclusive participation

Source: compiled by the author using [6]

The IRGC framework is uniquely equipped to handle "systemic risks" – the probability of breakdowns in entire systems (e.g., global financial systems, energy grids, or the biosphere) due to high connectivity and non-linear interactions. Systemic risks challenge established modes of governance that rely on compartmentalization [16]. They require "whole-of-society" approaches where insurers, banks, governments, and civil society coordinate using shared data and integrated models.

To understand why regulation varies across different policy domains, Christopher Hood, Henry Rothstein, and Robert Baldwin introduced the "risk regulation regime" approach [4]. A regime consists of the institutional geography, the rules, and the practices associated with a particular hazard. This meso-level analysis sits between society-wide theories (like Beck's) and single-case studies.

Components of a mentioned regime [4] include:

Institutional Geography: The organizational setup, which can be international, national, or local, and can range from single-agency control to fragmented, overlapping systems.

Rules: These vary in formality, from statutory codes to unwritten "club" rules, and in their targets (inputs, processes, or products).

Practice and Animating Ideas: The professional biases, the rigor of enforcement, and the preferred policy instruments (e.g., market incentives vs. command-and-control).

The variation in these regimes is typically explained by several forces [4]:

The Nature of the Hazard: Some risks require specialized expertise to recognize or are collective in impact, influencing the regime's complexity.

Market Failure Hypothesis: Regulation is often sized to correct market failures, such as externalities or information asymmetries.

Opinion-Responsive Government: Regimes are frequently shaped by public attitudes and media salience. Governments adjust regulation based on whether "lay" and "expert" views are aligned.

Interests and Lobbies: The distribution of power among business groups, NGOs, and professional experts significantly influences regime content.

Risk-oriented governance necessitates a departure from methodological monism. No single research method is inherently superior for studying the

e-ISSN 2786-5533

dynamics of the risk phenomenon. Instead, a plurality of quantitative and qualitative methods is required to bridge the gap between objective indicators and subjective contexts (Table 3).

Quantitative risk analysis relies on verifiable data and statistical models to measure probabilities and financial impacts. It is essential for cost-benefit analysis and the prioritization of risks in monetary terms. However, it is resource-intensive and can be rendered inconclusive by insufficient or poor data.

Qualitative risk analysis relies on expert judgment, experience, and descriptive tools like risk matrices or scenario planning. It is faster and captures contextual nuances, such as organizational culture or human factors, that quantitative models might overlook. While subjective, it provides the "subject-object" pluralism necessary for building consensus among diverse stakeholders [8].

In the context of policy evaluation, "Evidential Pluralism" (EBP+) advocates for integrating heterogeneous evidence [20]. This involves establishing both correlation (that a policy intervention causes an outcome) and mechanism (the underlying process that explains the correlation). EBP+ ensures that science is integrated into the policy process by scrutinizing mechanistic evidence alongside randomized controlled trials.

Table 3. Quantitative vs. Qualitative Risk Assessment

Aspect	Quantitative Risk Assessment	Qualitative Risk Assessment
Data Type	Numerical, Metrics, Verified Statistics	Descriptive, Expert Judgment, Experience
Key Tools	Monte Carlo simulations, CBA	Risk matrices, Scenario planning
Advantage	Objective, supports financial decisions	Fast, captures cultural & human factors
Disadvantage	Complex; needs high-quality data	Subjective; prone to assessor bias
Output	Numerical values (e.g., % probability)	Severity rankings (e.g., High/Med/Low)

Source: compiled by the author

A new approach – anticipatory governance – is the systemic capacity to act on a variety of inputs to manage emerging technologies and global

challenges while such management is still possible [18]. It requires a transformative shift from reactive to proactive institutions.

The OECD identifies five key dimensions (FIELD) and six enabling factors (SCOPES) for building anticipatory governance [19], given below.

Dimensions (FIELD):

Future-readiness: Ensuring the organization is prepared for various scenarios.

Innovation: The ability to develop new solutions for evolving challenges.

Endurance: Building resilience for policies to withstand long-term pressures.

Long-term perspective: Moving beyond short-term political cycles.

Direction: Establishing a clear sense of strategic purpose.

Enabling Factors (SCOPES):

Support from leadership: Commitment from top-level decision-makers.

Competencies: Developing specific skills within the workforce.

Observation of trends: Monitoring emerging changes and "weak signals".

Participatory processes: Engaging diverse stakeholders and the public.

Exchange of intelligence: Sharing data and good practices across silos.

Structures and procedures: Formal frameworks to integrate foresight into policy.

True institutional resilience is captured by the "AAA" framework: Antifragile, Anticipatory, and Agility [17]. Antifragility refers to systems that benefit and improve from shocks, focusing on the amplitude of potential consequences rather than just their probability. This requires organizational agility – the ability to recognize root causes and ready feasible options quickly – and a clear organizational "purpose" that acts as a North Star during crises.

In the planning of public infrastructure and policy, traditional Net Present Value (NPV) calculations are often insufficient because they assume investment decisions are "now-or-never" propositions. Real Options Theory (ROT) [9] offers a dynamic alternative, treating investment opportunities as options – the right, but not the obligation, to take action in the future.

Types of Real Options in Governance:

Option to Defer: The value of waiting for uncertainty to clear before committing to an irreversible expenditure.

Option to Expand: Designing systems today that can be scaled up if future demand is higher than expected.

Option to Abandon: The ability to stop a project to minimize losses if its value drops.

Switching Options: Designing flexibility into production or service systems to adapt to changing market conditions.

Incorporating real options maximizes the strategic value of public projects by providing the managerial flexibility to respond to uncertain environments.

As governance becomes more risk-oriented, the ethical framework of public administration must adapt. Accountability is shifting from *ex post* blame to *ex ante* responsibility, where public officials are encouraged to identify and manage risks proactively.

One of the primary risks of crisis-oriented governance is the "normalization of exceptional powers" [3]. Governments often justify temporary limitations on rights by invoking urgent threats (terrorism, migration, pandemics). This can lead to a "state of exception" where the boundary between emergency and norm becomes blurred, resulting in an expansion of executive authority at the expense of legislative and judicial oversight. Institutional actors must remain vigilant to ensure that extraordinary measures do not become a stable governing paradigm [4].

Ethical governance ensures transparency, integrity, and public trust, which are essential for the legitimacy of public institutions [1]. Public administration relies on a hierarchy of ethics: personal morality (the fundamental sense of right and wrong), professional ethics (standards specific to public service roles), and institutional ethics (codes of conduct and transparency mechanisms within agencies). Adhering to these principles ensures that public administrators prioritize collective welfare over narrow political or personal gain, even under the pressure of rapid change and uncertainty (*Table 4*).

e-ISSN 2786-5533

Table 4. Principles of Public Administration and their Role in Risk Governance

Principle	Role in Risk Governance	Outcome
Transparency	Open disclosure of risk data	Builds public trust and credibility
Accountability	Answerability for risk-taking	Deterrence of corruption and negligence
Meritocracy	Expert-led assessment	Enhances accuracy of technical analysis
Rule of Law	Legal constraints on emergency power	Prevents abuse of authority during crises

Source: compiled by the author using [1]

The mid-2020s have been defined by the emergence of the "Polycrisis" – a system of interconnected and compounding crises where risks from climate change, geopolitical conflict, pandemics, and technological disruption reinforce one another [10]. These crises challenge traditional emergency management that focuses on isolated events.

In a polycrisis, disruptions transmit through interconnected financial, logistics, and social systems. For instance, a climate-driven weather event can impact supply chains, pressure costs, and increase cyber exposure simultaneously. Because data drives modern systems, a single attack on a critical vendor can send shockwaves across an entire ecosystem [14].

Governance of the polycrisis requires "Integrated Risk Governance" – a proactive approach that replaces fragmented risk management with cross-sector collaboration [5]. This includes:

Shared Data and Common Resilience Goals: Insurers, banks, and regulators working together on joint stress-testing.

Network-Based Modeling: Capturing supply chain and ecosystem dependencies.

Ethically Defensible Trade-offs: Addressing conflicting societal goals (e.g., economic growth vs. climate stability) through inclusive participation.

Conclusions. This article has provided a comprehensive theoretical and methodological analysis of risk-oriented governance in contemporary public administration. The consolidation of risk-oriented governance within public administration theory and practice marks a fundamental shift in administrative

rationality. Reconceptualizing risk as a foundational category rather than a technical variable allows public institutions to develop the strategic capacity and institutional reflexivity necessary for the twenty-first century.

The findings of this analysis underscore the importance of:

1. Integrating Risk Governance: Moving beyond siloed departments to a holistic, "whole-of-government" approach where risk permeates the entire policy cycle.

2. Embracing Methodological Pluralism: Utilizing both quantitative precision and qualitative depth to capture the socio-cultural and indeterminate dimensions of risk.

3. Institutionalizing Anticipation: Building capacities for strategic foresight and experimentation to shift from reactive to proactive governance.

4. Strengthening Ethical Safeguards: Maintaining accountability and the rule of law to prevent the normalization of exceptional powers during crises.

5. Navigating the Polycrisis: Recognizing the systemic nature of contemporary risks and fostering global, cross-sectoral coordination to build shared resilience.

The evolution toward risk-oriented governance is not merely an administrative choice but a structural necessity for the survival and legitimacy of public institutions in an era of deep uncertainty and systemic vulnerability. The findings underscore the necessity of integrating risk-oriented governance into administrative reform, policy design, and institutional development. Future research should focus on comparative and longitudinal studies examining how different administrative systems institutionalize risk-oriented governance and how such approaches affect governance outcomes under uncertainty.

References:

1. Abdul Kader Jilani, M. M., Tasnim, S., Rahman, N., Asgar, A. S. M. R., & Ahmed, N. (2026). Role of ethics, meritocracy, and professionalism in public sector reforms: A Q methodology study. *PLoS one, 21(2),* e0342981. https://doi.org/10.1371/journal.pone.0342981.

2. Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.

3. Çobanoğlu, T. T. (2026). The Silent Erosion of Human Rights in Democratic Societies: Crisis Governance and the Normalization of Exceptional Powers. http://www.iconnectblog.com/the-silent-erosion-of-human-rights-in-democratic-societies-crisis-governance-and-the-normalization-of-exceptional-powers/.

4. Hood, Ch., Rothstein, H. & Baldwin R. (2003). *The Government of Risk: Understanding Risk Regulation Regimes.* Oxford Academic.

5. Hutton, H. (2025). Systemic Risk Governance. https://www.cisl.cam.ac.uk/news/systemic-risk-governance.

6. IRGC Risk Governance Framework (2019). https://irgc.org/risk-governance/irgc-risk-governance-framework/.

7. Jong, A. (2022). World Risk Society and Constructing Cosmopolitan Realities: A Bourdieusian Critique of Risk Society. *Front. Sociol.*, *7*, 797321. https://doi.org/10.3389/fsoc.2022.797321.

8. Kato, T. (2023). Well-being policy evaluation methodology based on WE pluralism. *Contemporary and Applied Philosophy, 14,* 159-175. https://doi.org/10.48550/arXiv.2305.04500.

9. Knudsen, O. K., & Scandizzo, P. L. (2011). Real Options and Project Evaluation: a Primer. https://documents1.worldbank.org/curated/en/300761468275362646/pdf/624870WP0P08720June090201100PUBLIC0.pdf.

10. Liu, H. & Renn, O. (2025). Polycrisis and Systemic Risk: Assessment, Governance, and Communication. *International Journal of Disaster Risk Science, 16,* 526–549. https://doi.org/10.1007/s13753-025-00636-3.

11. Oliveira, V. G. de, & Abib, G. (2023). Risk in public administration: A systematic review focused on a future research agenda. *Revista de Administração Pública*, *57*(6), e2022-0419. https://doi.org/10.1590/0034-761220220419x.

12. Osborne, S. P. (2006). The New Public Governance? *Public Management Review*, *8*(3), 377–387. https://doi.org/10.1080/14719030600853022.

13. Osborne, S. P. (Ed.). (2010). *The new public governance? Emerging perspectives on the theory and practice of public governance*. Routledge.

14. Parlov, N., Akrap, G. & Esterhajer, J. (2025). Supply Chain Security and AI Risk Governance Model for Critical Infrastructure under NIS2, CER, and CRA. *Applied Cybersecurity & Internet Governance, 4(1)*. https://doi.org/10.60097/ACIG/211823.

15. Renn, O. (2006). Risk Governance: An Application of Analytic-Deliberative Policy Making. in: VALDOR 2006. Values in Decisions on Risk, Stockholm, 14-18 May, 364–371.

16. Schweizer, P.-J., & Juhola, S. (2024). Navigating systemic risks: governance of and for systemic risks. *Global Sustainability*, *7*, e38. https://doi.org/10.1017/sus.2024.30.

17. Stephens, M., Awamleh, R., & Sicre, F. (Eds.). (2025). *Anticipatory Governance. Shaping a Responsible Future*. World Scientific.

18. Todisco, L., Mangia, G., Canonico, P. & Langella, F. (2025). Foreseeing the future: anticipatory governance as a response to the technological and managerial challenges in the public sector. *International Journal of Public Sector Management*, 1–17. https://doi.org/10.1108/IJPSM-03-2025-0109.

19. Tõnurist, P., & Orlik, J. (2025). Towards anticipatory governance guidelines for public sector organisations. OECD Working Papers on Public Governance, No. 82. OECD Publishing. https://doi.org/10.1787/a5203d0b-en.

20. Williamson, J. (2024). EBP+: Integrating science into policy evaluation using Evidential Pluralism. https://knowledge4policy.ec.europa.eu/blog/ebp-integrating-science-policy-evaluation-using-evidential-pluralism_en.

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: 27.03.26
Accepted: 26.05.26
Published: 26.06.26