UDC: 351.862.4:338.49-021.412.1(477)"364"

O. Batiuk

S. Pysarevskyi

O. Titov

BASIC PRINCIPLES OF SECURITY FOR CRITICAL INFRASTRUCTURE FACILITIES IN UKRAINE UNDER MARTIAL LAW

The article examines the legal acts of Ukraine, the European Union, and the United Kingdom on ensuring the security of critical infrastructure facilities. The views of domestic and foreign scholars on understanding the essence of the principles of critical infrastructure security and ways to implement them are studied.

The author identifies and analyses the following fundamental principles of critical infrastructure security in Ukraine during martial law: the principle of unity of methodological foundations; the principle of coordination; the principle of security, protection and safeguarding of restricted information; the principle of public-private partnership; the principle of coordination of efforts; the principle of complementary development; the principle of building integrated protection; the principle of international cooperation.

It is concluded that compliance with the fundamental principles of critical infrastructure security in Ukraine during martial law will ensure emergency preparedness, prevent future threats and respond effectively to emergencies related to the operation of critical infrastructure. This will create conditions for restoring its facilities, as well as minimising and eliminating the consequences of emergencies at these facilities or at facilities interacting with its operation.

***Keywords**: security, martial law, state, threats, measures, energy, infrastructure, facilities, principles.*

Statement of the problem. The relevance of the topic of ensuring the security of critical infrastructure facilities is considered to be a particularly important element of Ukraine's national security, covering a range of measures to protect, defend, defend and maintain the continuous operation of such facilities under martial law, in which Ukraine has been in since 5.30 a.m. on 24 February 2022 for a period of 30 days in accordance with the Decree of the President of Ukraine № 64/2022 of 24 February 2022 [1]. It is worth noting that today Ukraine is facing the largest security threats since its independence. A deep socio-political crisis unfolding in the context of external military interference in the internal affairs of the state is accompanied by an increase in extremist and terrorist manifestations, a rise in crime, including the use of firearms, a significant drop in economic indicators and a deepening humanitarian crisis in the eastern regions. The destruction and damage to a large number of businesses and infrastructure facilities have created a new security reality in which the protection of citizens, society and government institutions must be ensured.

Obviously, this situation raises the urgent need for a profound reform of the national security sector, considering international experience and the strategic course towards European integration. In this context, it is of particular importance to introduce the concept of critical infrastructure protection in Ukraine, which is widely used as a key instrument of modern security policy in the European Union, NATO and other leading countries.

It should be noted that in Ukraine, as in other countries, there are systems, facilities and resources whose destruction or damage can have significant negative consequences for citizens, society and state institutions. At the same time, it is incorrect to say that the issues of their protection and security are being ignored. On the contrary, there is a set of legislative and regulatory acts in place that govern the powers and competence of

the relevant state bodies, as well as define the specifics of organising the protection and ensuring the smooth functioning of these facilities and systems. However, we note that Ukraine currently lacks a holistic and systematic approach at the national level to managing the protection and security of a complex of systems, facilities and resources belonging to critical infrastructure. This leads to the dominance of departmental management methods, insufficient interaction and coordination between actors, and inefficient resource allocation, especially in national emergencies and martial law.

Analysis of recent research and publications. Many scholars, including S. Azarov [7], S. Belai [9], D. Biriukov [10], S. Bratel [11], V. Harmash [8], I. Hora [12], V. Kudriashov [13], have paid attention to scientific research on certain aspects of critical infrastructure security. The topics of their research concerned legal, economic, managerial, service and combat issues of critical infrastructure protection in Ukraine. This indicates an insufficient level of scientific research aimed at defining the fundamental principles of critical infrastructure security in Ukraine under martial law.

The purpose of the article is to study national and international regulatory and legal documents, to study the views of domestic and foreign scholars with a view to determining the fundamental principles of security of critical infrastructure facilities in Ukraine under martial law.

Summary of the main material. According to the official data of the Report on Direct Infrastructure Damage from Destruction as a Result of russia's Military Aggression against Ukraine, as of November 2024, since the beginning of the invasion, the total amount of direct damage to real estate, other infrastructure, vehicles and stocks has amounted to almost USD 170 billion. This is a significant amount. Compared to the previous estimate (as of the beginning of 2024), the amount increased by USD 12.6 billion (8 %) [6].

Total direct losses in the energy sector are estimated at USD 14.6 billion. The total direct losses in the energy sector are estimated at USD 14.6 billion. the total value of destroyed or damaged assets in industry, services and construction is USD 14.4 billion. The total value of destroyed or damaged assets in industry, services and construction is USD 14.4 billion. direct losses in the agricultural sector and land resources as a result of the hostilities amount to USD 10.3 billion. The total direct losses of the agricultural sector and land resources amounted to USD 10.3 billion. The total amount of direct damage to public sector facilities – including social infrastructure, educational, scientific, healthcare, cultural, sports and administrative buildings – is estimated at USD 16.3 billion (Table 1, Figure 1) [6].

Table 1 – General estimate of direct infrastructure damage as of November 2024

Type of property	Estimated direct losses, billion USD	Share, % of the total	Preliminary estimate, billion USD	Dynamics, % change
Residential buildings	60.0	35.3	58.9	1.9
Infrastructure	38.5	22.7	36.8	4.6
Energy sector	14.6	8.6	10.0	46.0
Assets of enterprises, industry	14.4	8.5	14.2	1.4
Agriculture and land resources	10.3	6.1	10.3	0.0
Education	7.3	4.3	7.4	– 0.8
Forestry fund	4.5	2.7	4.3	4.7
Health care	3.2	1.9	3.2	0.0
Culture, tourism, sports	2.5	1.5	2.1	20.0
Housing and communal servis	2.4	1.4	3.4	–29.4
Transport vehicles	2.0	1.2	1.6	25.0
Trade	1.2	0.7	1.2	0.0
Digital infrastructure	0.8	0.5	0.2	140.0
Administrative buildings	0.8	0.4	0.5	60.0
Social sphere	0.2	0.1	0.2	0.0
Financial sector	0.0	0.0	0.0	0.0
Total	169.8	100	157.2	8.0

Notes. KSE: heat indicators were transferred from housing and communal services to energy indicators, as CHP plants produce both electricity and heat. For comparison purposes, the transfer was also made for the preliminary assessment.

It is worth noting that in absolute terms, the largest increase in losses was recorded in the energy sector (over USD 4.6 billion), due to targeted attacks by the enemy on electricity generation and distribution facilities. Significant new losses were also observed in transport infrastructure, the social sphere, and among the production assets of enterprises. In relative terms, the highest growth rates of losses were recorded in administrative buildings (+60 %), energy infrastructure (+46 %), healthcare facilities (+32 %), and culture, tourism and sports (+29 %). The growth of losses in the digital infrastructure segment was even more pronounced, but these figures are not fully representative due to the lack of updated estimates in the previous report due to a lack of relevant data [6].

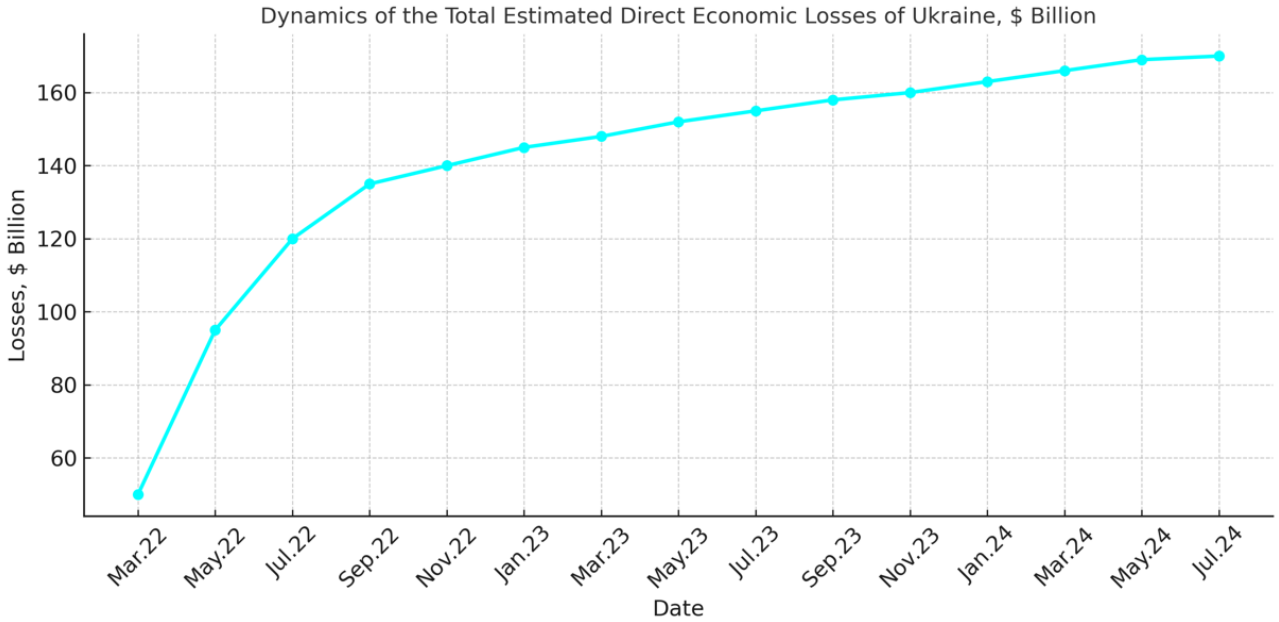

Figure 1 – Dynamics of the aggregate estimate of direct expenditures of the Ukrainian economy (in billion USD)

In geographical terms, the regions located in the immediate vicinity of the combat zone suffered the greatest losses (Figure 2). In particular, the ten regions that were temporarily occupied, border the russian federation or have access to the sea coast accounted for more than 90 % of the total direct losses. Given the enemy's systematic targeting of infrastructure facilities in regions relatively remote from the frontline, Dnipropetrovska oblast is also among the most affected areas [6].

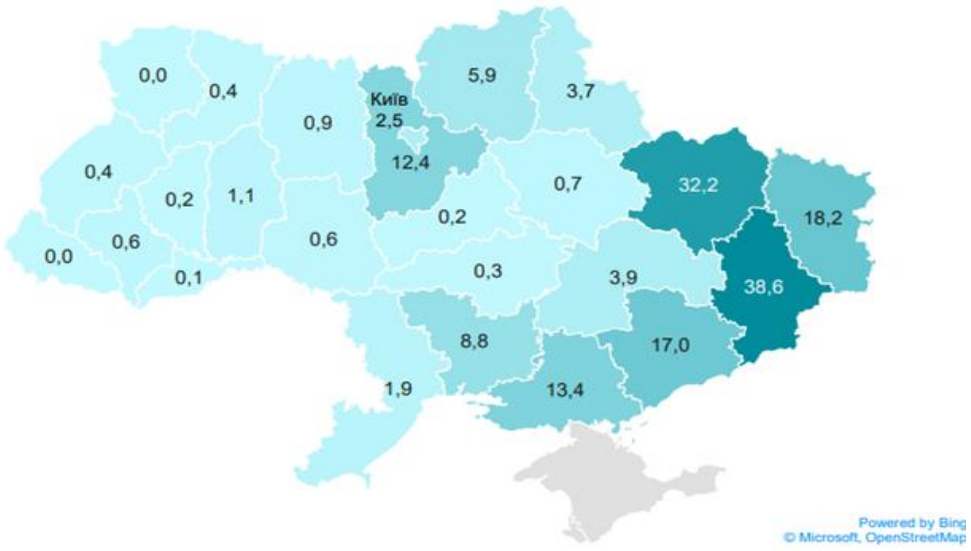

Figure 2 – Distribution of direct losses by region (in billion USD)

The above data demonstrates the relevance and necessity of studying the issues of protection of critical infrastructure during martial law in general and the study of the fundamental principles of critical infrastructure security in Ukraine under martial law in particular.

In addressing the topic of the fundamental principles of security of critical infrastructure facilities in Ukraine under martial law, we believe it is appropriate to first analyse the provisions of the current legislation of Ukraine. According to the Law of Ukraine "On National Security of Ukraine" of June 21, 2018 No. 2469-VIII (Art. 3) the main principles that determine the procedure for formulating state policy in the areas of national security and defence are: the rule of law, accountability, legality, transparency and compliance with the principles of democratic civilian control over the functioning of the security and defence sector and the use of force; compliance with international law, participation in the interests of Ukraine in international efforts to maintain peace and security, interstate systems and mechanisms of international collective security; development of the security and defence sector as the main instrument for the realisation of ehe Law of Ukraine "On Critical Infrastructure" (Art. 6) defines the basic principles of the national system of critical infrastructure protection as follows:

1) unity of methodological principles;
2) coordination;
3) public-private partnership;
4) security, protection and safeguarding of restricted information;
5) international cooperation [3].

Article 25 of the Law of Ukraine "On National Security of Ukraine" defines the purpose, principles and types of planning in the field of national security and defence. Planning in the areas of national security and defence is carried out in accordance with the following principles:

1) compliance with national legislation and international obligations of Ukraine;
2) democratic civilian control over the security and defence sector, openness of information on state policy, strategic documents, goals, priorities and tasks of planning, transparency and accountability of the use of resources;
3) integrity, coherence, systematic planning in the security and defence sector, considering the priorities and limitations set by state programmes, plans and forecast documents;
4) timeliness and compliance with the decisions taken to protect the national interests of Ukraine [2].

It should be noted that the protection of critical infrastructure should be understood as a set of measures implemented through regulatory, legal, organisational, technical and technological mechanisms and aimed at preventing threats, reducing risks, eliminating vulnerabilities, minimising negative consequences and ensuring the restoration of critical infrastructure in the event of emergencies (failures, accidents, etc.). In peacetime, these measures are aimed at ensuring the safety, security and stable operation of all critical infrastructure components: facilities, systems and networks (objects).

The fundamental principles of forming a critical infrastructure protection system are justified in accordance with the importance of ensuring national security in the modern state of Ukraine. We believe that the principles on which the protection of critical infrastructure should be based should be considered in the context of strategic security tasks.

In our opinion, the fundamental principles of forming a security system for critical infrastructure in Ukraine during martial law include the following.

The principle of unity of methodological foundations in the field of critical infrastructure security provides for the application of a unified, systematic and consistent methodology for analysing, planning, implementing and evaluating measures to ensure the protection of critical infrastructure. This principle ensures harmonisation of approaches to threat identification, risk assessment, development of security strategies and control over their implementation, which contributes to the effectiveness of the security system.

The implementation of the principle involves:

– the use of a unified conceptual and methodological framework for a comprehensive analysis of threats and vulnerabilities of critical infrastructure, covering man-made, natural, socio-political and military factors;

– integration of risk-oriented methods of analysis and forecasting to determine the priorities of measures to prevent and respond to threats;

– considering the peculiarities of the functioning of the protection system both in peacetime and in emergency situations and the state of emergency;

– coordination of regulatory, legal, organisational and technical instruments that ensure the implementation of security measures in cooperation between public and private actors;

– applying standardised procedures for threat assessment, certification of critical infrastructure facilities and monitoring their condition;

– ensuring unity of approach in planning human, technical, scientific and technical security.

Adherence to the principle of unity of methodological foundations ensures the integrity, coordination and adaptability of the critical infrastructure security system, which is a prerequisite for its effective functioning in the face of modern challenges.

The principle of coordination in the field of critical infrastructure security envisages coordinated, coordinated activities of all stakeholders – government agencies, the private sector, the public and the expert community – to effectively develop, implement and monitor measures to protect critical infrastructure facilities, ensure unity of action in strategic and operational security management, minimise duplication of functions, reduce the risks of fragmentation of responsibility and increase the efficiency of using existing and potential resources.

The principle of coordination is implemented in practice through:

– coordinated development of regulatory, legal, organisational, scientific and technological tools necessary to maintain an integral system of critical infrastructure protection;

– planning of security measures at the national level, considering strategic priorities for the protection of national interests;

– integration of critical infrastructure security issues into national programmes of socio-economic development and evaluation of their effectiveness;

– creation and functioning of a single coordination centre or platform responsible for assessing the state of security, forecasting threats and managing risks;

– centralised management of public and private resources to ensure their rational and efficient use in the face of threats;

– establishing mechanisms for horizontal (between executive authorities) and vertical (between central, regional and local levels) coordination of actions;

– ensuring transparency, information exchange and public participation through advisory structures.

Adherence to the principle of coordination contributes to the creation of a sustainable, adaptive and interdependent security system capable of effectively responding to modern complex threats to critical infrastructure.

The principle of security, protection and safeguarding of restricted information in the field of critical infrastructure security is to provide comprehensive protection against malicious acts and safeguard information on vulnerabilities, technical characteristics and features of physical protection systems of critical infrastructure against unauthorised access, except as provided by applicable law.

The implementation of the principle of security, protection and safeguarding of restricted information in practice involves:

– establishing clear rules and procedures for restricting access to information on vulnerabilities and characteristics of physical protection systems of critical infrastructure based on adopted regulatory documents;

– applying access control mechanisms, such as separation of user rights, multi-factor authentication and data encryption;

– training and raising awareness of staff on the importance of confidentiality and liability for disclosure of proprietary information;

– use of technical means of information protection, including information security systems, to prevent unauthorised access, leakage or loss of data;

– Ensuring legislative and regulatory regulation of the procedure for handling confidential information, as well as monitoring compliance with these rules;

– defining exceptional cases of information disclosure in accordance with applicable law and ensuring strict control in such cases.

The principle of public-private partnership in the area of critical infrastructure security involves the integration of all stakeholders involved in the operation of critical infrastructure facilities, with a clear delineation of areas of responsibility between them (in particular, the state as the owner, authorities as representatives of society, the regulator as the supervisory body, and the operator as the contractor).

The implementation of this principle should be based on the following key provisions:

– rational and integrated use of public and private sector resources to ensure effective protection of critical infrastructure;

– introducing the practice of officially declaring the level of security of the facility by its owner (operator), as well as certification of critical infrastructure facilities;

– ensuring participation of civil society and representatives of the expert community in the process of formulating requirements for the security of critical infrastructure, in particular through the establishment and functioning of advisory bodies.

The principle of coordination of efforts in the field of critical infrastructure security provides for systematic coordination of actions of all national security actors in order to achieve a holistic, effective and rational system of protection.

The content of this principle includes:

– harmonious development of the regulatory, legal, organisational, scientific and technological frameworks that ensure the implementation of tasks in the field of critical infrastructure protection;

– strategic security planning at the state level in accordance with national interests and through the development of mechanisms to influence the level of security of critical facilities;

– integration of critical infrastructure security issues into the processes of socio-economic planning, determination of state priorities and assessment of the country's development;

– creation and functioning of a centralised system for assessing the state of security, threat forecasting and risk analysis for critical infrastructure facilities;

– centralised management of available state resources for their optimal and targeted use in the security sector;

– defining and implementing a national scenario (projected threat) for critical infrastructure based on a comprehensive assessment of threats to national security.

The principle of complementary development in the field of critical infrastructure security is the consistent, complementary implementation of comprehensive measures that ensure the gradual improvement of the security and safety system. The application of this principle involves

– gradual introduction of regulatory, legal, organisational, scientific and technological tools that form the basis for improving the means and measures to protect critical infrastructure;

– development of methodological approaches to the identification and classification of critical infrastructure based on the analysis of available data;

– regular assessment of threats, risks and vulnerabilities of critical infrastructure facilities using best practices, including the experience of the nuclear industry and the banking sector;

– implementation of the results of scientific and applied research and long-term planning in the field of security, as well as the use of innovative high-tech solutions;

– strategic planning of human resources development, considering resources and capabilities of specialised educational institutions.

The principle of building comprehensive protection in the field of critical infrastructure security is to create a critical infrastructure protection system based on a unified methodological and conceptual framework for analysing threats, considering the complex impact of man-made, natural, socio-political and military factors.

This principle provides for consideration of the specifics of the functioning of protection both in peacetime and in emergency situations and the state of emergency. In addition, it gives priority to measures to prevent threats by applying risk-based methods of analysis and forecasting, which ensures effective prevention of emergencies and minimisation of their consequences.

The principle of international cooperation in the field of critical infrastructure security envisages systematic and active interaction of Ukraine with international organisations, platforms and partner states to ensure effective protection of national interests and enhancement of security. This principle is based on the integration of international standards, norms and agreements into national legislation, as well as practical measures that promote the harmonisation of policies and procedures in the field of civil protection, cybersecurity and counter-terrorism.

The implementation of the principle of international cooperation involves:

– Ukraine's active participation in international organisations and platforms that regulate civil protection, cybersecurity and counter-terrorism;

– implementation of international standards, norms and agreements into national legislation and practice in order to harmonise critical infrastructure protection measures;

– exchange of information and coordination of actions with other states to identify, assess and respond to cross-border threats and risks;

– joint exercises, trainings and operations with partners to improve preparedness and cooperation in emergency situations;

– development of intergovernmental mechanisms for rapid response and support in the event of crisis events that may have a transboundary nature;

– ensuring the participation of national experts in international research projects and exchange of experience in the field of critical infrastructure protection.

International regulations also define the principles of critical infrastructure security.

On 17 November 2005, the European Commission adopted a Green Paper on a European Critical Infrastructure Protection Programme, which envisaged the development of policy options aimed at establishing a coherent programme and a critical infrastructure warning network. The responses to the Green Paper pointed to the added value of the European Union's framework programme for the protection of critical infrastructure. The need to strengthen the capacity to protect critical infrastructure within the European Union and the importance of reducing its vulnerability to possible threats was emphasised. Particular attention is paid to compliance with the key principles of subsidiarity, proportionality, complementarity, and ensuring effective interaction between all stakeholders [5].

It is worth noting that the EU Council Directive of 8 December 2008 No. 2008/114/EC identifies and defines European critical infrastructure and assesses the need to improve their protection [4].

It is worth agreeing with scholars who believe that in the process of developing the national regulatory framework for the protection of critical infrastructure, special attention should be paid to documents that bring the requirements of national legislation as close as possible to the requirements for the operation and protection of critical infrastructure in the energy and transport sectors as defined in EU directives and specified in the EU-Ukraine Association Agreement. In particular, the following are mentioned:

– Directive No. 2005/89/EC on measures to ensure the security of electricity supply and investment in infrastructure;

– Directive No. 2004/67/EC on measures to ensure the continuity of supply of natural gas;

– Directive No. 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on strengthening the security of ports;

– Regulation (EC) No. 725/2004 of the European Parliament and of the Council of 31 March 2004 on the strengthening of the security of ships and port facilities;

– Directive No. 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on the safety of railways in the Community, amending Council Directive No. 96/18/EC on the licensing of railway undertakings and Directive No. 2001/14/EC on the unbundling of capacity on railway infrastructures and the charging of charges for the use of railway infrastructures and on safety certification (the Railway Safety Directive);

– Regulation (EC) No. 336/2006 of the European Parliament and of the Council of 15 February 2006 of on the implementation of the International Code of Conduct [5].

Conclusions

Having analysed the provisions of the current legislation of Ukraine, some EU countries and the UK, and having studied the positions of leading domestic and foreign scholars, we come to the following conclusions.

1. The fundamental principles of critical infrastructure security in Ukraine during martial law should include the following principles: unity of methodological foundations; coordination; security, protection and safeguarding of restricted information; public-private partnership; coordination of efforts; complementary development; building comprehensive protection; international cooperation.

2. Adherence to the fundamental principles of critical infrastructure security in Ukraine during martial law will minimise risks to the functioning of critical infrastructure, in particular, localisation and neutralisation of threats at the early stages of their occurrence.

3. In the event of emergencies at critical infrastructure facilities, the first priority should be to ensure the safety of the population and territories from the most dangerous radiological, chemical and bacteriological factors that may arise.

4. It is advisable to develop and implement engineering and technical civil protection measures to organise physical protection of critical infrastructure facilities, prevent unauthorised actions (including terrorist acts), mitigate the negative consequences of such actions and restore the functioning of facilities in case of their implementation.

5. Ensure protection of critical information infrastructure facilities from cyber-attacks, as well as protection of data and technical information contained in process control systems at critical infrastructure facilities from unauthorised blocking and modification.

6. In order to ensure the stable functioning of critical infrastructure in emergency situations and martial law, it is advisable to form material reserves, which should be preceded by an assessment and inventory of resources at critical infrastructure facilities.

Further research at will be aimed at studying the practical application of the fundamental principles of critical infrastructure security in Ukraine under martial law by the security and defence forces.

References

1. *Ukaz Prezydenta Ukrainy "Pro vvedennia voiennoho stanu v Ukraini" № 64/2022* [Decree of the President of Ukraine "On the introduction of martial law in Ukraine" activity no. 64/2022]. (2022, February 24). Retrieved from: https://www.president.gov.ua/documents/642022-41397 (accessed 1 May 2025) [in Ukrainian].

2. *Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" № 2469-VIII* [Law of Ukraine about the National Security of Ukraine activity no. 2469-VII]. (2018, June 21). Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed 1 May 2025) [in Ukrainian].

3. *Zakon Ukrainy "Pro krytychnu infrastrukturu" № 1882-IX* [Law of Ukraine about the Critical Infrastructure activity no. 1882-IX]. (2021, November 16). Retrieved from: https://zakon.rada.gov.ua/laws/show/1882-20#Text (accessed 1 May 2025) [in Ukrainian].

4. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). Retrieved from: https://www.legislation.gov.uk/eudr/2008/114/introduction (accessed 1 May 2025) [in English].

5. Natsionalnyi instytut stratehichnykh doslidzhen (2014). *Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini*. Kyiv, 2014. [Green Paper on Critical Infrastructure Protection in Ukraine]. Retrieved from: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf (accessed 1 May 2025) [in Ukrainian].

6. Andriienko D., Horiunov D., Hrudova V., Markuts Yu., Marshalok T., Neiter R., Piddubnyi I., Studennikova I., Topolskov D. (2025). *Zvit pro priami zbytky infrastruktury vid ruinuvan vnaslidok viiskovoi ahresii rosii proty Ukrainy stanom na lystopad 2024 roku* [Report on direct infrastructure losses from destruction caused by russia's military aggression against Ukraine as of November 2024]. Retrieved from: https://surl.li/hroeqr (accessed 1 May 2025) [in Ukrainian].

7. Azarov S. I., Sydorenko V. A., Yeremenko S. A., Pruskiy A. V., Demkiv A. M. (2021). *Zakhyst krytychnoi infrastruktury v umovakh nadzvychainykh sytuatsii* [Protection of critical infrastructure in emergency situations]. Kyiv [in Ukrainian].

8. Belai S., Lavrov I. (2023). *Teoretychni osnovy formuvannia systemy zahystu obiektiv krytychnoi infrastruktury v Ukraini* [Theoretical foundations for the formation of a system for protecting critical infrastructure in Ukraine]. *Chest i zakon*, no. 2 (85), pp. 5–11. DOI: https://doi.org/10.33405/2078-7480/2023/2/85/282518 [in Ukrainian].

9. Biriukov D. S. (2012). *Zakhyst krytychnoi infrastruktury: problemy ta perspektyvy vprovadzhennia v Ukraini* [Critical Infrastructure Protection: Problems and Prospects for Implementation in Ukraine]. Kyiv : FENIKS [in Ukrainian].

10. Bratel S. H. (2023). *Dosvid zarubizhnykh krain u sferi zabezpechennia bezpeky obiektiv krytychnoi infrastruktury* [Experience of foreign countries in the field of critical infrastructure security]. *Pivdennoukrainskyi pravnychyi chasopys*, no. 3, pp. 261–265. DOI: https://doi.org/10.32850/sulj.2023.3.41 [in Ukrainian].

11. Hora I. V., Batiuk O. V. (2021). *Okremi pytannia zakhystu obiektiv krytychnoi infrastruktury: zarubizhnyi dosvid* [Selected issues of critical infrastructure protection: foreign experience]. *Sotsialno-pravovi studii*, vol. 1 (11), pp. 132–139. Retrieved from: https://surl.li/bbffoa (accessed 1 May 2025) [in Ukrainian].

12. Kudriashov V. P. (2021). *Derzhavne rehuliuvannia krytychnoi infrastruktury* [State regulation of critical infrastructure]. *Finansy Ukrainy*, no. 7, pp. 72–92 [in Ukrainian].

The article was submitted to the editorial office on 20 May 2025

УДК: 351.862.4:338.49-021.412.1(477)"364"

О. В. Батюк, С. В. Писаревський, О. В. Тітов

ОСНОВОПОЛОЖНІ ПРИНЦИПИ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Досліджено нормативно-правові акти України, країн Європейського Союзу, а також Великої Британії щодо забезпечення безпеки об'єктів критичної інфраструктури. Вивчено погляди вітчизняних та іноземних науковців стосовно розуміння сутності принципів і шляхів їх реалізації щодо забезпечення безпеки об'єктів критичної інфраструктури.

Визначено доцільність проведення оцінювання загроз критичній інфраструктурі на національному рівні з урахуванням взаємозв'язків між окремими об'єктами та секторами інфраструктури, впливу зовнішніх чинників природного, соціально-політичного й техногенного характеру, а також оцінювання ризиків як на рівні окремих об'єктів, так і регіонів і держави загалом. Акцентовано на важливості розроблення та впровадження національної програми захисту критичної інфраструктури, необхідності запровадження функціонування мережі ситуаційних центрів, формування й ведення бази даних критичної інфраструктури, а також на проведенні постійної підтримки та координації роботи експертних і консультаційних рад різних рівнів у питаннях розроблення й упровадження нормативних, організаційних та технологічних заходів щодо захисту критичної інфраструктури. Вбачається доцільним розроблення планів реагування на надзвичайні ситуації та формування комплексної науково-дослідної програми у сфері захисту критичної інфраструктури з метою організації й подальшого здійснення співпраці зі структурами Європейського Союзу та державними органами країн-членів ЄС.

Отже, дотримання основоположних принципів безпеки об'єктів критичної інфраструктури в Україні у період воєнного стану дасть змогу забезпечити готовність до дій у надзвичайних ситуаціях, запобігти у майбутньому загрозам, а також забезпечуватиме ефективне реагування на надзвичайні події, пов'язані з функціонуванням критичної інфраструктури. Це сприятиме створенню умов для відновлення її об'єктів, а також мінімізації і ліквідації наслідків надзвичайних ситуацій на цих об'єктах або на об'єктах, що взаємодіють з її функціонуванням.

Ключові слова: *безпека, воєнний стан, держава, загрози, заходи, енергетика, інфраструктура, об'єкти, принципи.*

BATIUK Oleh – Doctor of Legal Sciences, Professor, Professor of the Department of National Security, Lesia Ukrainka Volyn National University
https://orcid.org/0000-0002-2291-4247

PYSAREVSKYI Serhii – Candidate of Sciences in Public Administration, Docent, Deputy Head of the Retraining and Professional Development Center, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-2537-0767

TITOV Oleh – Head of the Command and Control Training, Department Main Headquarters of the National Guard of Ukraine
https://orcid.org/0009-0004-4416-6843