

DOI 10.52363/2414-5866-2024-2-39

УДК 351.865:351.746.1

*Liashenko A., Student, National university of civil defence of Ukraine,  
Kharkiv, ORCID: 0009-0009-7566-1536*

*Zavada Y., Student, National university of civil defence of Ukraine,  
Kharkiv, ORCID: 0009-0008-1379-9751*

*Ляшенко А.Р., здобувачка вищої освіти, НУЦЗУ, м. Харків*

*Завада Є.Є., здобувачка вищої освіти, НУЦЗУ, м. Харків*

### PROSPECTS FOR ENSURING THE RESILIENCE OF CRITICAL INFRASTRUCTURE AND CIVIL SECURITY AT THE LOCAL LEVEL

### ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЦИВІЛЬНОЇ БЕЗПЕКИ НА МІСЦЕВОМУ РІВНІ

*The article explores the prospects for ensuring the stability of critical infrastructure at the local level in Ukraine in the context of guaranteeing its national security. It is revealed that the strategic level for ensuring the stability of critical infrastructure at the local level in Ukraine is the local one, as it is closest to the needs of the population and the performance of vital functions. The features of ensuring the stability of critical infrastructure abroad are analyzed.*

**Keywords:** *ensuring the stability of critical infrastructure, critical infrastructure facilities, public administration, national security, civil security, human resources, local programs, local level.*

*У статті досліджено перспективи забезпечення стійкості критичної інфраструктури на місцевому рівні в Україні в контексті гарантування її національної безпеки. Виявлено, що стратегічним рівнем забезпечення стійкості критичної інфраструктури на місцевому рівні в Україні є місцевий, адже він найбільш наближений до потреб населення та виконання життєво важливих функцій. Проаналізовано особливості забезпечення стійкості критичної інфраструктури за кордоном.*

**Ключові слова:** *забезпечення стійкості критичної інфраструктури, об'єкти критичної інфраструктури, публічне управління, національна безпека, цивільна безпека, кадровий потенціал, місцеві програми, місцевий рівень.*

**Problem setting.** One of the key factors of social development, ensuring the defense capability and economic security of states is infrastructure. This category was defined as "a complex of interconnected service structures or objects that constitute and provide the basis for the functioning of the system that ensures the operation of the armed forces" [6; 8]. Today, the concept of infrastructure has changed somewhat, but the most important essential feature has remained the same - infrastructure must ensure the satisfaction of the most important interests of the population, which can occur in various sub-areas. The provision of this infrastructure occurs at the central, regional and local levels. The latter is closest to the needs of the population, therefore it can be defined as strategic.

**Recent research and publications analysis.** The issues of public administration regarding the formation of public (public, civil) security and protection of critical infrastructure are the subject of both domestic and foreign scientists V. Andronov, K. Belikov, L. Berg, O. Boyko, A. Vodenicharov, S. Kaloyannidis, E.J. Kirshner, N. Klymenko, Y. Klyuchka, O. Kryukov, O. Leshchenko, P. Makhortov, O. Podskalna, S. Poteriyka, V. Terentyeva, O. Tverdokhlib, V. Zhu, M. Khoytink, etc. [1; 2; 8; 9].

**Paper objective.** The purpose of the article is to determine the prospects for ensuring the resilience of critical infrastructure and civil security at the local level.

**Paper main body.** The concept of "infrastructure" is one of the key ones in the development of various spheres of life. At the same time, "critical infrastructure" is the category around which the issues of the viability of all countries are built. The issues of conducting information confrontation are relevant today at the international level, within which many industries that are elements of critical infrastructure are involved [ibid.]. The definition of "critical infrastructure" is based on the concept of "criticality". In a number of definitions, this concept is applicable to that component of the category "infrastructure" that correlates with issues of security and the implementation of key functions. In engineering, criticality can be considered as a vector property of systems of various functional purposes in accordance with [9] "critical - the most important, decisive, determining". Criticality is determined taking into account the properties and functions of the object under study. The following components of criticality are distinguished: safety (reliability), effectiveness of consequences, the possibility of minimizing the probability of consequences [ibid.]. One of the indicators of criticality is structural criticality (importance, reliability).

In all term constructions, CI is recognized as a vital function of the services provided by an asset to society. Most countries define infrastructure as critical if its destruction would have nationwide consequences. However, the subject of impact varies slightly from country to country. For example, in the USA, the consequences of the destruction of critical infrastructure are directly related to national security and the safety of citizens and the economy. In the EU, the regional defini-

tion includes economic and social well-being. The NATO definition also includes any impact on the environment. Therefore, there are different approaches to defining the concept of CI. The results of the analysis of these definitions allowed us to characterize CI as the basic European definition at the international level, which is adhered to by the largest number of countries. In addition, the category of “critical information system” is currently actively developing [9].

It is worth noting that, despite the variety of approaches in defining CI, it was found that CI is significant at all levels of the state, which weakens the socio-economic effect of the development of society in the event of a CI disruption. This primarily makes the problem of ensuring the security of CI relevant, including, taking into account infrastructure dependencies and connections, at the level of the world community. The idea of conceptualizing issues of ensuring the security of critical infrastructure (hereinafter referred to as CI) is not new. The protection of strategic national resources and assets has been part of national defense planning since the Second World War. However, today, a significant influence on the perception of CI by Governments and ways to solve it is determined by security priorities, long-term development goals and financial considerations. Based on this, countries are trying to identify and protect their critically important assets from various threats. The starting point here is a coordinated state policy and legal environment.

In the EU, CI has been defined as an asset or system that is necessary to support vital societal functions (EU, 2008). As a result, a common approach to CI has been developed by EU member states (Table 1). Since 2013, the EU has been implementing a new approach to the European Critical Infrastructure Security Programme. The pilot project aims to optimise the protection and resilience of four selected European critical infrastructures: the European Organisation for the Safety of Air Navigation (Eurocontrol), Galileo – a global navigation infrastructure under civil control. The Directorate-General for Migration and Home Affairs is a structural unit of the European Commission and the lead organisation for the development of a critical infrastructure security plan within the European Commission [8].

The Joint Research Centre (JRC), the European Commission’s own research centre, supports assessment and analysis activities. The EU uses sectoral criteria for defining CIs. The criteria are set out in the European Certification of IT Professionals document, based on the severity of the consequences of a breach or disruption, which is assessed on the basis of societal impact, economic impact, environmental impact, and political impact. Once a CI is identified, its owners/operators take a specific set of actions to develop an Operator Security Plan. The CI Directive empowers the authorities in the Member States to be responsible for ensuring that CIs comply with its requirements. Each country's government chooses which specific body or bodies are responsible for implementing the CI system, for the proper incorporation of EU-level provisions into its national legislation [5].

Table 1

## Key policy and legal documents in the field of critical infrastructure protection in the EU [8]

Year	Document name	Brief description of the document
2003	European Security Strategy, 12 December 2003 (EU, 2003)	Defines the EU security environment, key security challenges and subsequent policy implications for the EU. Provides a conceptual framework for the common security and defence policy
2004	European Programme for Critical Infrastructure Protection (EPCIP) (EU, 2004)	A high-level document that sets out the basic principles of the BCI for the EU. It recognises and describes the threats that could lead to the loss of vital services
2006	Commission Communication on EPCIP of 12.12.2006 COM (2006) 786 final (EU, 2006)	Explanatory document on facilitating the implementation of EPCIP at the national level
2008	Directive 2008/114 on the identification of European critical infrastructures and the assessment of the need for their protection (EU, 2006)	Sets out the principles and procedures for the designation of a CI at EU level or a national CI that is recognised as a CI at EU level
2010	Stockholm Programme – An open and secure Europe serving and protecting citizens, 2010/C 115/01 (EU, 2010)	Formulates a roadmap for the EU's work for justice, freedom and security
2010	Communication from the Commission to the European Parliament and the Council on the EU Internal Security Strategy in Action: Five steps towards a more secure Europe, 22.11.2010 COM(2010) 673 final (EU, 2010a)	Identifies and addresses common threats to EU security, such as national disasters, criminal networks and radicalization
Supporting documents		
2012	EPCIP Review Commission Staff Working Document SWD(2012) 190 (EU, 2012a)	Summarizes the results of the review of the EPCIP and CIP Directives
2013	Commission Staff Working Document on a new approach to EPCIP, 28.8.2013 SWD (2013) 318 final (EU, 2013)	Establishes a new approach to EPCIP based on three core principles: prevention, preparedness and response

As for Ukraine, its legal framework is formed by special legislation - the Law of Ukraine "On Critical Infrastructure" (2021). Based on this law, the National Plan for the Protection and Ensuring the Security and Resilience of Critical

Infrastructure was approved. In addition, the State Service for Special Communications and Information Protection of Ukraine has developed methodological recommendations for the development of project threats to critical infrastructure at sectoral / object levels and the assessment of threats to critical infrastructure. Specialists of the Department of Critical Infrastructure Protection of the State Special Communications Administration, together with the Ministry of Development of Communities, Territories and Infrastructure of Ukraine, have prepared Methodological Recommendations for the development and approval of local programs to ensure the security and resilience of critical infrastructure and programs to increase the resilience of territorial communities to crisis situations. The development of these programs was approved by order of the Administration of the State Service for Special Communications dated November 30, 2023 No. 997 and is implemented within the framework of the National Plan for the Protection and Ensuring the Security and Resilience of Critical Infrastructure, approved by order of the Cabinet of Ministers of Ukraine dated September 19, 2023 No. 825-p.

Analysis of the provisions of these methodological recommendations allowed us to substantiate the directions for ensuring the sustainability of critical infrastructure at the local level. Local programs define goals and priorities aimed at protecting territorial communities and facilities that provide life for the population from threats. Among them are measures to ensure resilience to crisis situations, which include high-quality preparation, clear response and rapid recovery if necessary. The National Plan approved by the Cabinet of Ministers is a roadmap for planning in the field of critical infrastructure protection. It is very important that local authorities promptly get involved and develop their resilience programs in case of a crisis situation. According to the National Plan, local executive authorities (military-civilian administrations - if established) must develop and approve local programs to ensure the security and resilience of critical infrastructure, programs to increase the resilience of territorial communities to crisis situations caused by the termination or deterioration of the provision of services important for their vital activities or for the implementation of vital functions.

An analysis of the websites of local executive authorities (military-civilian administrations) revealed that not all of these bodies have developed and approved local programs to ensure the security and resilience of critical infrastructure, as well as programs to increase the resilience of territorial communities to crisis situations (Table 2). As can be seen from Table 2, as of today, local programs to ensure the resilience of critical infrastructure have been adopted in several regions of Ukraine. It was found that the programs are designed for a short-term period. It should be noted that there are regions where there is no local program at the regional level, but there is one in some of its territorial communities. It should also be noted that specific proposals for the protection of critical infrastructure are given in the programs of 3 regions (Chernivtsi, Chernihiv, and Zhytomyr Region).

Table 2

Functional map of critical infrastructure resilience software in the regions of Ukraine within the framework of relevant regional strategies, programs, plans

№ 3/п	Region name	Title of regional strategy, program, plan, etc. (with web link)	Means of ensuring the sustainability of the CI have been identified	No means of ensuring the sustainability of the CI have been identified
1.	Autonomous Republic of Crimea*	–	–	–
2.	Vinnitsia region	Program for Ensuring the Security and Resilience of Critical Infrastructure, Increasing Resilience to Crisis Situations for 2024-2026. URL: <a href="https://studenyanska-gromada.gov.ua/docs/1605177/">https://studenyanska-gromada.gov.ua/docs/1605177/</a> .		V (there is information about local programs in individual communities of the region)
3.	Volyn Region	Program for Ensuring the Security and Resilience of Critical Infrastructure, Increasing Resilience to Crisis Situations for 2024-2026. <a href="https://portal.nvrada.gov.ua/pro-zatverdzhennya-programy-zabezpechennya-bezpeky-ta-stijkosti-krytychnoyi-infrastruktury-pidvyshhennya-stijkosti-do-kryzovyh-sytuaczij-na-2024-2026-roky/">https://portal.nvrada.gov.ua/pro-zatverdzhennya-programy-zabezpechennya-bezpeky-ta-stijkosti-krytychnoyi-infrastruktury-pidvyshhennya-stijkosti-do-kryzovyh-sytuaczij-na-2024-2026-roky/</a> .		V (there is information about local programs in individual communities of the region)
4.	Dnipropetrovsk Region	Program for Increasing the Resilience of the Pokrovska Urban Territorial Community to Crisis Situations. URL: <a href="https://pkrv.dp.gov.ua/documents/download/dodatok_do_programi_pidvischennya_stijkosti_do_krizovyh_situacij_ed6fedb29f2a368a7a326af1f2751407.docx">https://pkrv.dp.gov.ua/documents/download/dodatok_do_programi_pidvischennya_stijkosti_do_krizovyh_situacij_ed6fedb29f2a368a7a326af1f2751407.docx</a> .		V (there is information about local programs in individual communities of the region)
5.	Donetsk Region *	–	–	–
6.	Zhytomyr Region	Program for Increasing the Resilience of the Zhytomyr Urban Territorial Community to Crisis Situations for 2024-2026. URL: <a href="https://ztrada.gov.ua/?pages=18406">https://ztrada.gov.ua/?pages=18406</a>	<b>V</b>	
7.	Zakarpattia Region	Integrated Program for Civil Defense of Zakarpattia Region for 2020-2024. URL: <a href="https://oda.carpathia.gov.ua/dokument/pro-kompleksnu-programu-rozvytku-cyvilnogo-zahystu-zakarpatskoyi-oblasti-na-2020-2024-0">https://oda.carpathia.gov.ua/dokument/pro-kompleksnu-programu-rozvytku-cyvilnogo-zahystu-zakarpatskoyi-oblasti-na-2020-2024-0</a> .		V (there is information about local programs in individual communities of the region)
8.	Zaporizhia Region	Regional Civil Defense Program Zaporizhia Region for 2021-2025. URL: <a href="http://depczn.zoda.gov.ua/?page_id=282">http://depczn.zoda.gov.ua/?page_id=282</a>		V

		.		
9.	Ivano-Frankivsk Region	Regional Civil Protection Program Ivano-Frankivsk Region for 2022-2025. URL: <a href="https://www.if.gov.ua/regionalnicilovi-programi/programi-upravlinnyaz-pitan-civilnogo-zahistu">https://www.if.gov.ua/regionalnicilovi-programi/programi-upravlinnyaz-pitan-civilnogo-zahistu</a>		V (there is information about local programs in individual communities of the region)
10.	Kyiv Region	Regional Program for Civil Defense of Kyiv Region for 2024-2027. URL: <a href="https://kor.gov.ua/wp-content/uploads/2023/12/Dodatok-35.pdf">https://kor.gov.ua/wp-content/uploads/2023/12/Dodatok-35.pdf</a>		V
11.	Kirovograd region	Regional Program for Civil Defense of Kirovohrad Region for 2022-2027. URL: <a href="https://www.oblrada.kr.ua/decission/2897/-pro-zatverdzhennya-oblasnoiprogrami-tsivilnogo-zahistukirovogradskoi-oblasti-na-2022-2027-roki--07-12-2021">https://www.oblrada.kr.ua/decission/2897/-pro-zatverdzhennya-oblasnoiprogrami-tsivilnogo-zahistukirovogradskoi-oblasti-na-2022-2027-roki--07-12-2021</a> .		V
12.	Luhansk region *	–	–	–
13.	Lviv Region	Comprehensive Program for Civil Protection of Lviv Region. URL: <a href="https://old.loda.gov.ua/upload/users_files/25/upload/Zvit%20pro%20vYkonannya%20Kompleksna%20programa%20cYvil_nogo%20zahYstu%20naseleennya%20i%20terYtoriy%20L_vivs_koi%20oblasti%20vid%20nadvYchaynYh%20sYtuaciy%20tehnogenного%20ta%20prYrodnogo%20harakteru.pdf">https://old.loda.gov.ua/upload/users_files/25/upload/Zvit%20pro%20vYkonannya%20Kompleksna%20programa%20cYvil_nogo%20zahYstu%20naseleennya%20i%20terYtoriy%20L_vivs_koi%20oblasti%20vid%20nadvYchaynYh%20sYtuaciy%20tehnogenного%20ta%20prYrodnogo%20harakteru.pdf</a>		V
14.	Mykolaiv Region	Program for Increasing the Resilience of the Bilopol Urban Territorial Community to Crisis Situations. URL: <a href="https://bilopillya-meria.gov.ua/docs/1494780/">https://bilopillya-meria.gov.ua/docs/1494780/</a>		V (there is information about local programs in individual communities of the region)
15.	Odesa Region	Civil Protection Program of the Odessa Region for the Period 2022-2025. URL: <a href="https://oblrada.od.gov.ua/wp-content/uploads/416-VIII.pdf">https://oblrada.od.gov.ua/wp-content/uploads/416-VIII.pdf</a>		V
16.	Poltava Region	Civil Protection Program of Poltava Region for the Period 2021-2027. URL: <a href="https://oblrada-pl.gov.ua/sites/default/files/field/docs/16_9.pdf">https://oblrada-pl.gov.ua/sites/default/files/field/docs/16_9.pdf</a> .		V
17.	Rivne Region	Program for Increasing the Resilience of the Bereznivka Territorial Community to Crisis Situations. URL: <a href="https://berezne-miskrada.gov.ua/cilovi-programi-08-42-51-16-05-2024/">https://berezne-miskrada.gov.ua/cilovi-programi-08-42-51-16-05-2024/</a> .		V (there is information about local programs in individual communities of the region)
18.	Sumy Region	Target Program for the Protection of the		V

		Population and Territory of the Sumy Urban Territorial Community from Emergencies of a Technogenic, Natural and Military Nature for 2022-2024. URL: <a href="https://smr.gov.ua/images/documents/Nakaz_SMVA/2024/04_Kviten/191_SMR_24.04.2024/191_SMR_dod.docx">https://smr.gov.ua/images/documents/Nakaz_SMVA/2024/04_Kviten/191_SMR_24.04.2024/191_SMR_dod.docx</a>		
19.	Ternopil Region	Civil Protection Program of the Ternopil Region for the Period 2023-2027. URL: <a href="https://oda.te.gov.ua/diyalnist/regionalnicilovi-programi">https://oda.te.gov.ua/diyalnist/regionalnicilovi-programi</a>		V
20.	Kharkiv Region	Regional Targeted Program for the Development of Civil Protection of the Kharkiv Region for 2021-2023. URL: <a href="https://kharkivoda.gov.ua/oblasnaderzhavna-administratsiya/struktura-administratsiyi/strukturnipidrozdzili/717/102538">https://kharkivoda.gov.ua/oblasnaderzhavna-administratsiya/struktura-administratsiyi/strukturnipidrozdzili/717/102538</a> .		V
21.	Kherson Region	Program for the Prevention and Elimination of Emergencies (Accidents) and Rapid Response to Them in the Kherson Region. URL: <a href="https://khoda.gov.ua/perel%D1%96k-regionalnyh-tsilyovyh-program">https://khoda.gov.ua/perel%D1%96k-regionalnyh-tsilyovyh-program</a> .		V
22.	Khmelnyskyi Region	Program for the Prevention and Elimination of Emergencies (Accidents) and Rapid Response to Them in the Khmelnytskyi Region. URL: <a href="https://kmo-blrada.gov.ua/wp-content/uploads/2019/02/dodatok-do-rish-programa.doc">https://kmo-blrada.gov.ua/wp-content/uploads/2019/02/dodatok-do-rish-programa.doc</a> .		V
23.	Cherkasy Region	Target Program for Ensuring the Resilience of the Kaniv Urban Territorial Community to Crisis Situations for 2024-2027. URL: <a href="https://kaniv-rada.gov.ua/docs/1623323/">https://kaniv-rada.gov.ua/docs/1623323/</a>		V (there is information about local programs in individual communities of the region)
24.	Chernivtsi Region	A Comprehensive Program for Ensuring the Security and Resilience of Critical Infrastructure of the Chernivtsi Region for 2023-2025. URL: <a href="https://bukoda.gov.ua/storage/app/uploads/public/651/6bd/7b6/6516bd7b6db18677208332.pdf">https://bukoda.gov.ua/storage/app/uploads/public/651/6bd/7b6/6516bd7b6db18677208332.pdf</a>	V	
25.	Chernihiv Region	Program for Ensuring the Security and Resilience of Critical Infrastructure of the Chernihiv Region for 2023-2024. URL: <a href="https://dcz.cg.gov.ua/index.php?id=39354&amp;tp=1">https://dcz.cg.gov.ua/index.php?id=39354&amp;tp=1</a>	V	

\* excluding the Autonomous Republic of Crimea, Donetsk and Luhansk regions



In addition, it was found that the existing local programs in the field of ensuring the resilience of critical infrastructure are of the same type. Although this should not be the case, since each community is unique in size, population, infrastructure, etc., which is influenced to varying degrees by external and internal factors. The state of functioning of frontline territorial communities, deoccupied communities and those located in the central and western parts of Ukraine is different. At the same time, the functioning of territorial communities should be aimed at providing services important to society under any conditions (both in peacetime and under martial law) [7].

**Conclusions of the research.** Thus, we can conclude that Ukraine has not yet formed the necessary legal framework in the field of ensuring the resilience of critical infrastructure, in particular at the local level. It has been established that not all local government bodies have developed and approved programs to ensure the resilience of critical infrastructure within their individual communities. In this context, it is insisted that the task of the relevant bodies is to resolve this issue, since the level of security of critical infrastructure partly depends on it.

Ensuring the security and stability of critical infrastructure has become one of the most pressing issues for our state today. This is due not only to the resolution of the war against Ukraine, but also to the dynamics of social, economic, political and even technological processes taking place in the world. Trends in the intensification of threats of a natural and man-made nature, the increase in the level of terrorist threats, the increase in the number and complexity of cyberattacks, as well as damage to infrastructure facilities as a result of the armed aggression of the Russian Federation, make the issue of protecting systems, facilities and resources that are critically important for the functioning of society, the socio-economic development of the state and ensuring national security more urgent.

#### References:

1. Andreytsev, V.V. (2019), "Subject composition of activities related to objects of increased danger: economic and legal aspects", *Ekonomika ta pravo*, vol. 3, pp. 39–48.
2. Boyko, O.A. (2023), "Objects of increased danger: introduction of improved approaches to their identification", *Tsyvil'nyy zakhyst ta pozhezhna bezpeka*, vol. 1 (15), pp. 83–91.
3. Zdolbunivska City Council. Program for ensuring the security and resilience of critical infrastructure. URL: <https://zdgromada.gov.ua/wp-content/uploads/2023/10/1.-pro-shvalennya-proyektu-programy-zabezpechennya-bezpeky-ta-stijkosti-krytychnoyi-infrastruktury.docx>. (Accessed 26 Oct 2024).
4. Pomaza-Ponomarenko, A.L. and Moroz, S.A. (2023), "Civil defense as a sphere of ensuring the national security of Ukraine", *Zbirka dopovidej na Vseukayins'koyi naukovo-praktychnij konferentsii* [Conference Proceedings of the All-Ukrainian Scientific and Practical Conference], National University, Zhytomyr, Ukraine, pp. 305–308.

5. Pomaza-Ponomarenko, A.L. and Taraduda, D.V. (2024), “Ensuring the stability of the system of state regulation of increased danger facilities and critical infrastructure facilities”, *Derzhavne upravlinnya: udoskonalennya ta rozvytok*, vol. 4. available at: <https://www.nayka.com.ua/index.php/dy/article/view/3461> (Accessed 26 Oct 2024).
6. Pomaza-Ponomarenko, A.L. and Taraduda, D.V. (2024), “Mechanisms for ensuring civil security of Ukraine: aspects of emergency prevention at the facilities of the military-industrial complex”, *Publichne administruvannya ta natsional'na bezpeka*, vol. 3 (44). available at: <https://www.inter-nauka.com/issues/administration2024/3/9732> (Accessed 26 Oct 2024).
7. Methodological recommendations for the development of project threats to critical infrastructure at sectoral/object levels and the assessment of threats to critical infrastructure. URL: [https://moz.gov.ua/uploads/ckeditor/%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%B0%20%D1%96%D0%BD%D1%84%D1%80%D0%B0/19-12-2023/1/%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%20%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%2056781.pdf?\\_\\_cf\\_chl\\_tk=ZIOST.BiTEDLEjbSMe7TqTge pIobemCvoRUpkI7CK2Y-1726124035-0.0.1.1-8937](https://moz.gov.ua/uploads/ckeditor/%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%B0%20%D1%96%D0%BD%D1%84%D1%80%D0%B0/19-12-2023/1/%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%20%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%2056781.pdf?__cf_chl_tk=ZIOST.BiTEDLEjbSMe7TqTge pIobemCvoRUpkI7CK2Y-1726124035-0.0.1.1-8937).
8. Klaver, M.H.A., Luijff, H.A.M., Nieuwenhuijs, A.H., Cavenne, F., Ulisse, A. and Bridgeman, G. (2008), “European risk assessment methodology for critical infrastructures”, *2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future*, IEEE, Piscataway, New Jersey, USA, 10-12 November 2008, pp. 1–5.
9. Nakamura, E.T., Silva, J.A. and Rios, J.M.M. “Mobile Telecommunications Networks for the 2014 World Cup”, available at: <https://www.gsma.com/latinamerica/wp-content/uploads/2012/06/WorldCup2014-CPqD.pdf> (Accessed 26 Oct 2024).
10. Pomaza-Ponomarenko, A., Taraduda, D., Leonenko, N., Poroka, S. and Sukhachov, M. (2024), “Ensuring the safety of citizens in times of war: aspects of the organization of civil defense”, *AD ALTA: Journal of Interdisciplinary Research*, vol. 14, issue 1, pp. 216–220.
11. Popov, O., Taraduda, D., Sobyna, V., Dement, M. and Pomaza-Ponomarenko, A. (2020), “Emergencies at Potentially Dangerous Objects Causing Atmosphere Pollution: Peculiarities of Chemically Hazardous Substances Migration”, *Systems, Decisions and Control in Energy I. Studies in Systems, Decision and Control*, Switzerland: Springer International Publishing AG, vol. 298, pp. 151–163.
12. The Spanish Security Strategy (2011), “Everyone’s Responsibility. Gobierno de Espana”, available at: <https://publications.hse.ru/en/chapters/78410684> (Accessed 26 Oct 2024).

#### **Список використаних джерел:**

1. Андрейцев В.В. Суб’єктний склад діяльності, пов’язаної з об’єктами підвищеної небезпеки: господарсько-правові аспекти // *Економіка та право*. 2019. № 3. С. 39–48.
2. Бойко О.А. Об’єкти підвищеної небезпеки: упровадження вдосконалених підходів до їх ідентифікації // *Цивільний захист та пожежна безпека*. 2023. 348

№ 1 (15). С. 83–91.

3. Здолбунівська міська рада. Програма забезпечення безпеки та стійкості критичної інфраструктури. URL: <https://zdgromada.gov.ua/wp-content/uploads/2023/10/1.-pro-shvalennya-proyektu-programy-zabezpechennya-bezpeky-ta-stijkosti-krytychnoyi-infrastruktury.docx>.

4. Помаза-Пономаренко А.Л., Мороз С.А. Цивільний захист як сфера забезпечення національної безпеки України // Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття : Матеріали Всеукр. науково-прак. конф. (07-08.12.2023 р., м. Житомир). С. 305–308.

5. Помаза-Пономаренко А.Л., Тарадуда Д.В. Забезпечення стійкості системи державного регулювання об'єктів підвищеної небезпеки // Державне управління: удосконалення та розвиток. 2024. № 4. URL: <https://www.nauka.com.ua/index.php/dy/article/view/3461>.

6. Помаза-Пономаренко А.Л., Тарадуда Д.В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). URL: <https://www.inter-nauka.com/issues/administration2024/3/9732> (дата звернення 26.10.2024).

7. Методичні рекомендації щодо розробки проектних загроз критичній інфраструктурі секторального\об'єктового рівнів та оцінки загроз критичній інфраструктурі. URL: [https://moz.gov.ua/uploads/ckeditor/%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%B0%20%D1%96%D0%BD%D1%84%D1%80%D0%B0/19-12-2023/1/%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%20%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%2056781.pdf?\\_\\_cf\\_chl\\_tk=ZI0ST.BiTEDLEjbsMe7TqTgepIobemCvoRUpkI7CK2Y-1726124035-0.0.1.1-8937](https://moz.gov.ua/uploads/ckeditor/%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%B0%20%D1%96%D0%BD%D1%84%D1%80%D0%B0/19-12-2023/1/%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%20%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%2056781.pdf?__cf_chl_tk=ZI0ST.BiTEDLEjbsMe7TqTgepIobemCvoRUpkI7CK2Y-1726124035-0.0.1.1-8937).

8. Klaver M.H.A., Luijff H.A.M., Nieuwenhuijs A.H., Cavenne F., Ulisse A., Bridgeman G. European risk assessment methodology for critical infrastructures // 2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future, IEEE, Piscataway, New Jersey, USA, 10-12 Nov. 2008, pp. 1–5.

9. Nakamura E.T., Silva J.A., Rios J.M.M. Mobile Telecommunications Networks for the 2014 World Cup. URL: <https://www.gsma.com/latinamerica/wp-content/uploads/2012/06/WorldCup2014-CPqD.pdf>.

10. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Vol. 14. Issue 1. Pp. 216–220.

11. Popov O., Taraduda D., Sobyna V., Dement M., Pomaza-Ponomarenko A. (2020). Emergencies at Potentially Dangerous Objects Causing Atmosphere Pollution: Peculiarities of Chemically Hazardous Substances Migration. Systems, Decisions and Control in Energy I. Studies in Systems, Decision and Control. Switzerland: Springer International Publishing AG. Vol. 298. P. 151–163.

12. The Spanish Security Strategy 2011. Everyone's Responsibility. Gobierno de Espana. URL: <https://publications.hse.ru/en/chapters/78410684>.