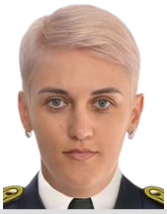
UDC 351.746:351.861:005.334(477)

V. Torichny

V. Zalogh



I. Shashkun

ANALYSIS OF THREATS AND RISKS TO CRITICAL INFRASTRUCTURE FACILITIES OF THE STATE BORDER SERVICE OF UKRAINE

The article provides a systematic analysis of threats and risks affecting critical infrastructure facilities of the State Border Service of Ukraine. It substantiates the relevance of ensuring the stability of critically important facilities of the border agency, on which border security, the state's defence capability, and the stability of management, communication, logistics and life support systems directly depend, both in everyday conditions and under special legal regimes. It is revealed that modern threats to critical infrastructure facilities of the State Border Service of Ukraine are complex and multidimensional in nature and include military, terrorist, man-made, cybernetic, information-psychological and socio-economic factors.

The results obtained allow us to determine the priorities for protecting critical infrastructure facilities, optimise the allocation of resources and form the basis for building an integrated risk management system in the State Border Service of Ukraine. The proposed approach provides the opportunity to identify vulnerable elements in a timely manner, predict threats, and develop preventive and compensatory measures. The practical implementation of the research results will be an important condition for increasing the resilience of the critical infrastructure of the border agency, ensuring its continuous and effective functioning both in everyday conditions and under special legal regimes.

Keywords: *State Border Service of Ukraine, state border, border security, organisational resilience, critical infrastructure, facility protection, threats, risks, analysis, classification, risk management, governance.*

Statement of the problem. The events of the last decade in Ukraine, namely the armed aggression of the Russian Federation (hereinafter referred to as the RF) and the introduction of martial law in 2022, have led to a significant increase in the range of threats that undermine the border security and defence capability of the state, its socio-economic stability and other vital national interests. In the current conditions of large-scale war, the issue of ensuring the stability and security of critical infrastructure facilities (hereinafter referred to as CIF) in the security and defence sector (hereinafter referred to as SDS), in particular the State Border Guard Service of Ukraine (hereinafter referred to as the SBGS), which plays a key role in ensuring the security and protection of the state border (hereinafter referred to as the SB), maintaining the country's defence capabilities and the stability of the integrated state border management system of Ukraine.

The critical infrastructure of the SBGS is an integral part of the national security system, as it ensures the performance of tasks in the integrated management system of Ukraine's state border, the organisational stability of management systems, communications, information and logistics networks, etc. Threats directed against such objects are complex in nature and combine military, terrorist, cyber, information and psychological, man-made and other factors. Their implementation can lead to a violation of the organisational stability of management systems, loss of functional capacity of the State Border Guard Service, reduction in the effectiveness of operational and service activities (hereinafter referred to as OSA) and destabilisation of work in general.

In the current environment, there has been a significant increase in the level of threats directed specifically at the critical infrastructure of the border agency. These threats are characterised by high dynamics of manifestation, complexity of forecasting and potentially serious consequences.

At the same time, the specific nature of the State Border Guard Service's activities entails particular risks related to the geographical location of facilities, the degree of their engineering protection, the level of technical equipment and dependence on external communications and supplies. Given the situation described above, there is an urgent need to create a scientifically based system for identifying, classifying and analysing threats and risks to critical infrastructure facilities of the State Border Guard Service. This will allow for the timely

identification of vulnerable elements, assessment of risk levels, and development of effective mechanisms for preventing and minimising negative consequences.

Solving this problem through scientific means will contribute to the improvement of legal, organisational and technical measures to protect critical infrastructure facilities of the State Border Guard Service, increase its organisational stability, especially in conditions of special legal regimes, and ensure the continuity of management activities. In view of the above, conducting research dedicated to analysing threats and risks to critical infrastructure facilities of the State Border Guard Service of Ukraine is relevant, timely and a logical continuation of the authors' previous research.

Analysis of recent research and publications. The issue of ensuring the security of critical infrastructure has long been one of the priority areas of research for Ukrainian scientists. An analysis of recent publications on this topic [1–12] shows a steady increase in attention to critical infrastructure protection issues in the context of national security, particularly in the context of the introduction of special legal regimes. This interest is driven by the need to ensure the stability of state institutions, components of the SDS and their management systems in the face of constant hybrid threats.

Despite the significant number of scientific works devoted to the problems of state critical infrastructure security, the issues of comprehensive and systematic analysis of threats and risks to critical infrastructure facilities of the State Border Service of Ukraine remain insufficiently researched. Scientific publications by specialists [13–14] consider certain aspects of the problem, in particular, the analysis of risks and the development of a methodological framework for their assessment in conditions of martial law. At the same time, such studies are mostly fragmentary in nature and do not form a comprehensive scientific concept for assessing threats and risks in different conditions of the State Border Guard Service's operation.

There is still no systematic approach that would combine risk analysis in the everyday conditions of the State Border Guard Service and in conditions of special legal regimes, which significantly complicates the formation of an effective critical infrastructure security management system. In this context, it is important to conduct research aimed at identifying, systematising and assessing potential threats and risks to critical infrastructure facilities of the border agency, as well as developing an analytical basis for building risk management models. The results obtained will be of great practical importance – they will contribute to increasing the level of stability of the functioning of the critical infrastructure of the State Border Guard Service in its daily activities and under special legal regimes.

The purpose of the article is to conduct a systematic analysis of threats and risks to critical infrastructure facilities of the State Border Guard Service in the context of everyday activities and special legal regimes for the purpose of their further identification, assessment and management within the risk management system.

Summary of the main material. Critical infrastructure of the State Border Guard Service is considered in the article as a set of facilities, their parts and systems that are important for ensuring border security and managing the state border of Ukraine, the disruption of which could harm the vital national interests of the state and have a significant negative impact on national security, defence and the functioning of society [18].

The functioning of such objects is accompanied by a wide range of threats of various kinds. In this context, it is advisable to analyse existing classifications of threats to critical infrastructure and, based on the results of such an analysis, propose an author's classification of threats. Such research is of practical importance for the development of effective measures to counteract and protect the critical infrastructure of the State Border Service of Ukraine in the current conditions.

An analysis of foreign experience shows that the classification of threats to critical infrastructure in different countries has both common features and significant national differences, which is due to the specifics of the security situation, state policy priorities and the level of infrastructure development. Thus, in the United States, threats are defined as natural or man-made phenomena, entities or actions that can cause harm to life, information, property, etc., with priority attention focused on cyberattacks, terrorist acts and natural disasters.

In European Union countries, the approach to threat classification is based on the principles of the European Programme for Critical Infrastructure Protection, which identifies cyber threats, terrorism, criminal acts, man-made accidents and natural hazards. Germany offers a more detailed classification that covers natural phenomena (floods, storms, droughts, earthquakes, avalanches, etc.), human error and technical failures, as well as terrorist acts and criminal activities aimed at disrupting the functioning of critical infrastructure. In France and the United Kingdom, the emphasis is on cyber threats and terrorist acts, with specialised agencies coordinating countermeasures and analysing intelligence data. In Northern and Eastern European countries, particularly Denmark and the Netherlands, CCI threats are viewed through the prism of emergencies, accidents

and crisis management, while in Romania the classification is based on natural, accidental and intentional threats [15].

This experience shows that, regardless of the specific country, the classification of threats to critical infrastructure is based on a systematic approach that takes into account the sources of threats, their types and their potential impact on the functioning of critical infrastructure facilities. At the same time, specific approaches to identifying and prioritising threats are developed taking into account national specifics, the security situation and the technological characteristics of the state. For Ukraine, and in particular for the critical infrastructure facilities of the State Border Guard Service, aspects related to modern military aggression, missile and drone strikes, sabotage, cyber threats, and information and psychological influences are important.

Based on international approaches and the specifics of the functioning of the State Border Guard Service, it is advisable to identify the main categories of threats and risks of their realisation, taking into account both traditional sources of danger (natural, man-made, criminal) and modern factors of military and hybrid influence.

Table 1 presents the author's classification of threats to critical infrastructure facilities of the State Border Guard Service, which will serve as an analytical basis for risk assessment and risk management system development.

Table 1 – Classification of threats to critical infrastructure facilities of the State Border Guard Service of Ukraine

Category of threats	Typical scenarios (vectors) of threat realisation	Nature of impact on the CIF of the State Border Service
1	2	3
Military and political threats	Missile and drone strikes, artillery shelling, occupation of territories with important infrastructure, disruption of logistics supply chains, etc.	Physical destruction of structures and equipment of strategic importance for the security and defence capability of the state, damage to personnel, disruption of continuity of functions, logistics, destabilisation of the situation in the country, etc.
Terrorist and sabotage threats	Physical attacks on border guards, checkpoints, planting of explosive devices or arson, sabotage of transport and energy infrastructure in the border area	Disabling facilities, disrupting operations, causing local destruction, creating panic and undermining trust in state authorities, etc.
Natural and climatic threats	Natural disasters (earthquakes, floods, storms, hurricanes, landslides, forest fires), climate change, epidemics and pandemics	Damage to infrastructure, physical integrity of structures, complications in movement and supply, threats to the life and health of personnel (reduced working capacity), reduced staffing levels (due to illness or injury), disruption (damage) to communications, etc.
Operational threats	Natural wear and tear of engineering structures and communications, failure or malfunction of equipment due to violations of technical maintenance regulations, non-compliance with operating rules, personnel errors during maintenance or operation, use of poor-quality materials or components, lack of backup systems or insufficient level of their readiness	Partial or complete failure of critical infrastructure elements, reduced efficiency of life support systems, communications, energy supply, interruption or reduced stability of facilities, increased repair and restoration costs, increased risk of accidents, fires or other man-made emergencies
Man-made threats	Man-made accidents at energy facilities, leaks of hazardous substances, explosions, fires at production facilities; technical failures, transport disruptions; failures in communication, water and heat supply systems, etc.	Loss of power supply, disruption of transport and logistics links, failures in control systems, failure of technical systems, etc.

End of Table 1

1	2	3
Cyber threats	Hacker interference, cyberattacks on information and communication systems, DDoS attacks, malicious software, data theft or destruction, manipulation of automatic control systems	Unauthorised alteration or distortion of information (data integrity), access to confidential information, disruption of management systems, data loss, disorganisation of management processes, distribution of malicious software, etc.
Criminal (criminal) threats	Destruction of border infrastructure, attacks (capture) of service facilities and deployment points	Violation of the legal regime of the border, violation of the security of facilities and personnel, destabilisation of logistics, loss of material resources, complications in control, etc.
Information and communication threats	Information and psychological operations (IPO), disinformation, propaganda, psychological pressure on personnel	Compromising reputation and undermining public trust, destabilising the work of units, reducing the morale of personnel, erroneous decisions, internal destabilisation, panic, etc.
Socio-economic threats	Corruption, underfunding, staff shortages, rising energy or fuel costs, budget cuts for infrastructure maintenance, dependence on imports of critical materials, financial crimes (fraud, money laundering, other illegal financial transactions)	Disruption of the continuity of CIF operations, increased operating costs, non-compliance with safety and maintenance standards due to resource constraints, leading to a cascade of operational and man-made threats, complications in the implementation of projects and tasks, limitations on the modernisation and maintenance of CFI, etc.
Management (administrative and organisational) threats	Absence or inconsistency of emergency response plans, insufficient coordination between management bodies, services and departments, deficiencies in the internal control system, low qualifications of personnel, staff shortages, violations of security management or response procedures.	Reduced effectiveness of security systems, delayed or inadequate response to incidents, increased likelihood of other threats materialising, loss of control over units in crisis situations, etc.

The proposed classification of threats to critical infrastructure facilities of the State Border Guard Service is based on a comprehensive analysis of the current challenges faced by the state and the border agency directly. Its relevance lies in its ability to provide a comprehensive approach to threat analysis, covering both traditional and contemporary factors arising in the context of martial law and hybrid warfare. This approach is based on the principles of systematicity, comprehensiveness, analysis of cause-and-effect relationships, adaptability, and relevance to the border sphere. It allows not only to systematise threats and take into account all possible aspects of their impact on critical infrastructure objects of the State Border Guard Service, but also to effectively allocate resources to prevent and neutralise negative consequences.

At the same time, for the practical application of the analysis, it is also necessary to analyse the risks, which will allow assessing the probability of specific threats materialising and the potential scale of their impact.

Such an analysis serves as the basis for building a risk management system, developing preventive measures, and setting priorities in ensuring the security of the border agency's critical infrastructure.

In previous studies [16], the authors developed a classification of CIF based on the following key characteristics: functional purpose; level of criticality (importance for functioning); degree of vulnerability and nature of threats; spatial and territorial characteristics; type of resources ensuring functioning; types of potential threats; degree of protection.

It should also be noted that in studies devoted to the management of CIF risks, it is expedient and methodologically correct, in the authors' opinion, to use the same or similar names for categories of threats

and corresponding categories of risks. This approach is based on the logical connection between sources of potential danger and the possible negative consequences of their realisation. In this context, a threat is considered to be an event or set of conditions that may have an undesirable impact on CIF, while risk is defined as the probability of this threat being realised in combination with the scale of possible consequences.

That is why the authors of the article synchronised the names of the categories: for example, military-political threats correspond to military-political risks, man-made threats to man-made risks, cyber threats to cyber risks, etc. Such terminological consistency simplifies the structuring of analytical materials and ensures the logical unity of the classification. At the same time, it is important to emphasise that the coincidence of names does not mean the identity of content: a threat describes a potential impact, while a risk characterises the possibility and expected consequences of this impact. Thus, the use of identical categories of threats and risks is justified, increases the structure of the analytical process and ensures the methodological compatibility of the risk management model in the State Border Guard Service system.

Based on the results of the analysis, it is possible to summarise them in the form of a matrix "risk object – types of risks – importance for functioning – criticality category" (Table 2).

Table 2 – Risk matrix for critical infrastructure objects of the State Border Guard Service

Objects of risk	Types of risks	Criticality category in accordance with regulatory documents [17], [18]
Engineering and technical structures of the state border	Military-political; terrorist and sabotage; natural and climatic; operational; man-made; criminal (criminal)	II (vital)
Technical means of state border protection	cyber risks; operational; natural and climatic; military and political	II (vital)
Communication systems	cyber risks; information and communication; military-political, terrorist; sabotage	I particularly (critically) important
Management and control objects	cyber risks; military-political; terrorist; sabotage; organisational; operational	I particularly (critically) important
Logistical objects	military-political; terrorist; sabotage; organisational; man-made; operational; socio-economic	II (vital)
Life support facilities	military-political; terrorist; sabotage; organisational; man-made; operational; natural and climatic	II (vital)
Security facilities	terrorist; sabotage; criminal (criminal); military-political; man-made; organisational	II (vital)
Logistical support facilities	military-political; terrorist; sabotage; man-made; operational; socio-economic; organisational	III important
Social infrastructure facilities	military-political; terrorist; sabotage; socio-economic, operational; man-made	IV necessary

Analysis of the above matrix allows us to draw a number of general conclusions about the structure of risks, categories of criticality and priorities for managing the security of critical infrastructure facilities of the State Border Service of Ukraine.

1. General risk structure. The critical infrastructure facilities of the State Border Guard Service of Ukraine have a complex, multi-level risk structure that covers virtually all categories defined by the classification. The most common are:

– military and political risks – characteristic of all facilities without exception, reflecting the current state of military threat and armed aggression against Ukraine;

– terrorist and sabotage threats – present in the vast majority of facilities, in particular in the system of security and protection of critical infrastructure, management and logistics;

– operational and man-made risks – inherent in engineering, technical, logistical and rear facilities, indicating the need for enhanced technical control, maintenance and modernisation;

– cyber risks and information security risks – concentrated in communication, management and technical control systems, i.e. in segments that ensure the stability of the management circuit of the State Border Guard Service.

2. Main patterns and trends:

– the highest density of military-political, man-made, sabotage and terrorist risks is observed at the level of I-II categories of criticality of facilities, which determines the priority of their protection;

– there is a stable interdependence of risks of various natures. For example, the destruction of facilities as a result of hostilities (military-political threat) can provoke man-made accidents or communication disruptions (cyber risks, information risks);

– organisational risks have a significant impact on the stability of Category II–III facilities, especially in terms of logistics, resource management and coordination between departments.

– risks with a lower criticality category (III–IV) act as a multiplier of the overall vulnerability of the system, as their cumulative effect can reduce the ability to respond quickly and restore critical elements.

Conclusions

The study found that the issue of risk analysis in the field of critical infrastructure protection of the State Border Guard Service of Ukraine is insufficiently developed in the scientific community, despite its particular relevance. The study confirmed that the critical infrastructure of the State Border Guard Service of Ukraine is a system-forming element, on whose resilience and security the effectiveness of the protection and defence of critical infrastructure depends.

The main categories of threats and risks have been identified, which are complex in nature and cover military-political, sabotage, terrorist, man-made, cyber, information, socio-economic and organisational factors.

The most critical impact is exerted by military-political, terrorist, sabotage, man-made and operational risks, the realisation of which could cause a systemic disruption of the State Border Guard Service's functioning. The study clarifies the essence of the concepts of "threat" and "risk" as basic elements of the critical infrastructure security management system.

The proposed classification of threats and risk matrix will enable systematic assessment of the criticality of objects and determination of priorities for their protection depending on their importance for the functioning of the agency and the state as a whole.

The results of the analysis confirm the need to create an integrated risk management system in the State Border Guard Service, which would provide for continuous monitoring, assessment, prevention and minimisation of the consequences of the realisation of threats. The practical implementation of the research results will contribute to increasing the resilience of the critical infrastructure of the State Border Guard Service and the integrated management system of Ukraine's state border, both in everyday conditions and under special legal regimes.

References

1. Hora I. V., Batyuk O. V. (2021). *Okremi pytannya zakhystu ob'yektiv krytychnoyi infrastruktury: zarubizhnyy dosvid* [Certain issues of protection of critical infrastructure facilities: foreign experience]. *Sotsial'no-pravovi studiyi,* no.1(11), pp. 132 –139. Retrieved from: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3709/1/18-.pdf. (accessed: 21 June 2025) [in Ukrainian].

2. Biriukov D. S., Kondratov S. I. (2016). *Zelena knyha z pytan' zakhystu krytychnoyi infrastruktury v Ukrayini* [Green Book on Issues of Critical Infrastructure Protection in Ukraine]: *zbirnyk mizhnarodnykh ekspertnykh narad.* Kyiv: NISD. 176 p. Retrieved from: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf (accessed: 24 June 2025) [in Ukrainian].

3. Biriukov D. S., Kondratov S. I. (2012). *Stratehiia zakhystu krytychnoyi infrastruktury v systemi natsional'noyi bezpeky derzhavy* [Strategy of Critical Infrastructure Protection within National Security System of the State]. *Stratehichni priorytety*, no. 3, pp. 107–113. Retrieved from: https://www.researchgate.net/publication/301698438_Strategy_of_Critical_Infrastructure_Protection_within_National_Security_System_of_the_State (accessed: 21 June 2025) [in Ukrainian].

4. Uriadnikova I. V., Zaplatynskyi V. M. (2020). *Naukovi pidkhody do vyznachennia terminu «krytychna infrastruktura»* [Scientific Approaches to the Definition of the Term "Critical Infrastructure"]. *Visti Donets'koho hirnychoho instytutu*, no. 2 (47). DOI: https://doi.org/10.31474/1999-981X-2020-2-184-193. [in Ukrainian].

5. Franchuk V. I., Pryhunov P. Ya., Melnyk S. I. (2021). *Bezpeka ob'iektiv krytychnoyi infrastruktury v Ukrayini: orhanizatsiino-normatyvni problemy ta pidkhody* [Security of Critical Infrastructure Facilities in Ukraine: Organizational and Regulatory Problems and Approaches]. *Sotsial'no-pravovi studii*, no. 3 (13), pp. 142–148. Retrieved from: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf (accessed: 25 June 2025) [in Ukrainian].

6. Havrys' A. P., Filippova V. V., Tur N. Yu. (2024). *Informatsiinyi analiz system zakhystu ob'iektiv krytychnoyi infrastruktury v period dii voiennoho stanu* [Information Analysis of Critical Infrastructure Protection Systems during Martial Law]. *Visnyk LDUBZhD*, no. 30, pp. 173–187. DOI: https://doi.org/10.32447/20784643.30.2024.17 [in Ukrainian].

7. Verholyas O. O. (2020). *Reformuvannya systemy zakhystu ta pidvyshchennya stiykosti krytychnoyi infrastruktury Ukrayini v rozrizi aktual'nykh zahroz* [Reforming the protection system and increasing the resilience of critical infrastructure in Ukraine in the context of current threats]. Retrieved from: https://coolyanews.info/reformuvannya-sistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriizii-aktual.html (accessed: 10 October 2025) [in Ukrainian].

8. Bobro D. H. (2015). *Vyznachennya kryteriyiv otsinky ta zahrozy krytychniy infrastrukturi* [Determining the criteria for assessing and threatening critical infrastructure]. *Stratehichni priorytety. Seriya: Ekonomika,* no. 4, pp. 83–93 [in Ukrainian].

9. Yermenchuk O. P. (2018). *Otsinka zahroz krytychniy infrastrukturi yak vazhlyva skladova chastyny diyal'nosti iz zakhystu derzhavnoyi bezpeky* [Assessment of threats to critical infrastructure as an important component of state security protection activities]. *Natsional'nyy yurydychnyy zhurnal: teoriya i praktyk,* pp. 50-54. Retrieved from: https://ibn.idsi.md/ sites/default/files/imag_file/50-54_4.pdf (accessed: 30 October 2025) [in Ukrainian].

10. Sukhodolya O. M. (2016). *Zakhyst krytychnoyi infrastruktury v umovakh hibrydnoyi viyny: problemy ta priorytety derzhavnoyi polityky Ukrayiny* [Critical infrastructure protection in hybrid warfare: problems and priorities of state policy of Ukraine]. *Stratehichni priorytety. Seriya: Polityka,* no. 3 (40), pp. 65–67 [in Ukrainian].

11. Murasov R., Nikitin A., Meshcheryakov I., Pidhorodets'kyy M., Poplavets' S. (2024). *Metodyka otsinyuvannya zahroz i ryzykiv dlya ob"yektiv krytychnoyi infrastruktury za stsenariyamy rozvytku nadzvychaynykh sytuatsiy* [Methodology for assessing threats and risks for critical infrastructure facilities according to emergency scenarios]. *Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony,* no. 48(3), pp. 35–43. DOI: https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [in Ukrainian].

12. Ivanyuta S. P., Panov YE. M., Ivanenko O. I., Hapon S. V. (2024). *Otsinka ryzykiv krytychniy infrastrukturi Ukrayiny v umovakh rosiys'koyi viys'kovoyi ahresiyi* [Risk assessment for critical infrastructure of Ukraine in conditions of Russian military aggression]. *Visnyk NTUU "KPI imeni Ihorya Sikors'koho". Seriya: Khimichna inzheneriya, ekolohiya ta resursozberezhennya,* no.2, pp. 47–61. DOI: https://doi.org/10.20535/2617-9741.2.2024.307360 [in Ukrainian].

13. Zalozh V. V., Torychnyi V. O., Hluzdan' O. P. (2025). *Analiz ryzykiv u sferi zakhystu krytychnoi infrastruktury Derzhavnoi prykordonnoi sluzhby Ukrainy v umovakh voiennoho stanu* [Risk analysis in the field of critical infrastructure protection of the State Border Guard Service of Ukraine under martial law]. *Natsionalni interesy Ukrainy: naukovo-praktychniy zhurnal*, no. 8(13), pp. 130-141. DOI: https://doi.org/10.52058/3041-1793-2025-8(13)-130-141 [in Ukrainian].

14. Zalozh V. V., Torichnyy V. O., Hluzdan' O. P., Antokh O. V. (2025). *Model' otsinyuvannya ryzykiv u sferi krytychnoyi infrastruktury Derzhavnoyi prykordonnoyi sluzhby Ukrayiny v umovakh voyennoho stanu* [Model of risk assessment in the critical infrastructure sector of the State Border Service of Ukraine under

martial law]. *Natsional'ni interesy Ukrayiny: naukovo-praktychnyy zhurnal,* no. 9(14), pp. 176-193. DOI: https://doi.org/10.52058/3041-1793-2025-9(14)-176-193 [in Ukrainian].

15. Herasymenko O. M. (2024). *Zahrozy ob"yektam krytychnoyi infrastruktury Ukrayiny v umovakh voyennoho stanu* [Threats to critical infrastructure facilities of Ukraine under martial law]. *Naukovyy visnyk Uzhhorods'koho Natsional'noho Universytetu: seriya Pravo,* no. 3(84), pp. 257-263. DOI: https://doi.org/10.24144/2307-3322.2024.84.3.39 [in Ukrainian].

16. Torichnyy V. O., Zalozh V. V., Shashkun I. V. (2025). *Analiz ta klasyfikatsiya ob"yektiv krytychnoyi infrastruktury Derzhavnoyi prykordonnoyi sluzhby Ukrayiny* [Analysis and classification of critical infrastructure facilities of the State Border Guard Service of Ukraine]. *Natsional'ni interesy Ukrayiny: naukovo-praktychnyy zhurnal,* no. 11(16), pp. 510-520. DOI: https://doi.org/10.52058/3041-1793-2025-11(16)-510-520 [in Ukrainian].

17. *Rozporiadzhennia Kabinetu Ministriv Ukrainy "Pro skhvalennia Kontseptsii stvorennia derzhavnoyi systemy zakhystu krytychnoyi infrastruktury" № 1009-r* [On approval of the Concept for creating a state system for the protection of critical infrastructure: Order of the Cabinet of Ministers of Ukraine no. 1009-r]. (2017, December 6) Retrieved from: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (accessed: 27 June 2025) [in Ukrainian].

18. *Zakon Ukrainy "Pro krytychnu infrastrukturu" № 1882-IX* [Law of Ukraine On Critical Infrastructure no. 1882-IX] (2021, November 16]. *Verkhovna Rada of Ukraine*. Retrieved from: https://zakon.rada.gov.ua/laws/show/1882-20#Text (accessed: 05 June 2025) [in Ukrainian].

The article was submitted to the editorial office on 17 November 2025

УДК 351.746:351.861:005.334(477)

В. О. Торічний, В. В. Залож, І. В. Шашкун

АНАЛІЗ ЗАГРОЗ І РИЗИКІВ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

У статті здійснено системний аналіз загроз і ризиків, що впливають на об'єкти критичної інфраструктури Державної прикордонної служби України. Обґрунтовано актуальність проблеми забезпечення стійкості функціонування критично важливих об'єктів прикордонного відомства в повсякденних умовах та в умовах особливих правових режимів, від яких безпосередньо залежить прикордонна безпека, обороноздатність держави, стабільність систем управління, зв'язку, логістики та життєзабезпечення. Розкрито, що сучасні загрози для об'єктів критичної інфраструктури Державної прикордонної служби України мають комплексний, багатовимірний характер і включають воєнні, терористичні, техногенні, кібернетичні, інформаційно-психологічні та соціально-економічні чинники прояву.

Проаналізовано наукові джерела з проблематики безпеки критичної інфраструктури та виявлено недостатній рівень комплексності в підходах до оцінювання ризиків саме у прикордонній сфері. Наголошено, що існує потреба у створенні цілісного підходу до аналізу загроз і ризиків для об'єктів критичної інфраструктури Державної прикордонної служби України, який б поєднував аспекти повсякденної діяльності та функціонування в умовах особливих правових режимів.

У межах дослідження уточнено сутність понять «загроза» та «ризик» як базових елементів системи управління безпекою критичної інфраструктури. Запропоновано авторську класифікацію загроз для об'єктів критичної інфраструктури ДПСУ. Для кожної категорії визначено типові сценарії їх реалізації та характер впливу. Класифікація базується на принципах системності, комплексності, адаптивності й практичної спрямованості та враховує міжнародний досвід захисту критичної інфраструктури.

Розроблено узагальнену матрицю ризиків об'єктів критичної інфраструктури Державної прикордонної служби України, у якій систематизовано типові категорії ризиків за об'єктами та визначено рівні їх критичності. Аналіз матриці засвідчив домінування воєнно-політичних, терористичних, диверсійних, кібернетичних та експлуатаційних ризиків, реалізація яких може

спричинити порушення організаційної стійкості системи управління та зниження ефективності оперативно-службової діяльності.

Отримані результати дозволяють визначити пріоритети захисту об'єктів критичної інфраструктури, оптимізувати розподіл ресурсів та формувати основу для побудови інтегрованої системи управління ризиками в Державній прикордонній службі України. Запропонований підхід забезпечує можливість своєчасного виявлення уразливих елементів, прогнозування загроз, розроблення превентивних і компенсаційних заходів. Практичне впровадження результатів дослідження стане важливим чинником підвищення стійкості критичної інфраструктури прикордонного відомства, забезпечуючи її безперервне та ефективне функціонування як у повсякденних умовах, так і за дії особливих правових режимів.

Ключові слова: *Державна прикордонна служба України, державний кордон, прикордонна безпека, організаційна стійкість, критична інфраструктура, захист об'єктів, загрози, ризики, аналіз, класифікація, ризик-менеджмент, управління.*

Torichnyi Vadym – Doctor of Science in Public Administration, Associate Professor, Professor of the Department of Management, National Academy of the State Border Guard Service of Ukraine
https://orcid.org/0000-0003-3336-6386

Zalozh Viktor – Candidate of Military Sciences, Associate Professor, Honored Worker of Education of Ukraine, Associate Professor of the Department of Management, National Academy of the State Border Guard Service
https://orcid.org/0000-0001-8974-8661

Shashkun Iryna – Adjunct, National Academy of the State Border Guard Service of Ukraine
https://orcid.org/0009-0002-5355-5248