**UDC 351.865**

**O. Nazarenko**

**O. Holovan**

**V. Rudynskyi**

# ON THE ISSUE OF ASSESSING THE VULNERABILITY OF CRITICAL INFRASTRUCTURE OBJECTS IN WARTIME CONDITIONS

*The issue of protecting critical infrastructure becomes a top priority under wartime conditions. Infrastructure of strategic significance includes facilities, systems, and networks, the uninterrupted operation of which is vital to the functioning of the state, the economy, and citizens' well-being. Evaluating the vulnerability of such entities enables the identification of weak points in the security system, prevention of potential attacks, and provision of effective response planning in the context of national security.*

*The authors propose a scientifically grounded approach to assessing the vulnerability of critical infrastructure objects in Ukraine during martial law, considering contemporary threats (military, cyber, subversive).*

***Keywords:*** *critical infrastructure objects, vulnerabilities, risks, threats.*

**Statement of the problem.** Critical infrastructure objects (CIOs) are key elements ensuring the stable functioning of the government, society, economy, and national security. These strategic assets appear as primary targets for the opponent, prompting the need for their reliable protection and timely response to emerging threats. First and foremost, it is important to assess their vulnerability to identify weak points at an early stage, enhance protection measures, and rapidly mitigate possible hazards.

The use of high-tech means of attack, including unmanned aerial vehicles (UAVs), electronic warfare equipment, and large-scale cyberattacks, significantly increases the risk level for critical infrastructure components. Consequently, assessing the vulnerability of such facilities gains particular importance, allowing the identification of potential security gaps within the defense system, prioritizing protective measures, and formulating effective response strategies.

Despite the relevance of that issue, the methodology for determining CIO vulnerability in Ukraine currently requires improvement and adaptation to wartime conditions. Existing approaches are fragmented and occasionally outdated, having been originally developed for peacetime scenarios. Additionally, the practical implementation of infrastructure protection measures often lacks a systematic character, which decreases the overall national security level.

Therefore, an immediate need arises for developing a scientifically grounded approach to CIO susceptibility assessment. This approach must consider the specifics of contemporary military threats, incorporate interdisciplinary analysis methods, and provide a foundation for informed decision-making in the sphere of state safety. Within the modern context, estimation of the sensitivity of critical infrastructure facilities becomes especially relevant.

**Analysis of recent research and publications.** A review of regulatory documents, scientific sources, and literature regarding vulnerability assessment, the protection situation, and potential threats to critical infrastructure objects, particularly in Ukraine, has been conducted. Directive [1] establishes the procedure for the sensitivity check of nuclear facilities and radioactive materials. Order [2] approves the methodology, criteria, and indicators for assessing the security status of emergency authorities concerning epidemics, cybersecurity, and determining the protection level against economic terrorism. Criteria for evaluating pivotal infrastructure risks are defined in a scientific article [3]. The authors of the study [4] propose a technique for estimating danger and threats to emergency objects under enemy fire impact. Article [5] discusses the methods for assessing threats and risks to CIOs under emergency scenarios. The methodology for determining cyberspace protection of critical facilities is introduced in the paper [6].

These publications cover various evaluative aspects of CIOs, including identification methods, risk management, cybersecurity, and the use of contemporary technologies for monitoring and defense. However, policy documents and studies [1–6] insufficiently address the issues of CIO sensibility checking under martial law.

**The purpose of the article** is to enhance a scientifically based approach to assessing the vulnerability of Ukraine's critical infrastructure facilities under wartime conditions, considering contemporary threats (military, cyber, and subversive).

The following specific research tasks have been addressed to achieve the specified goal: analyzing the current state of the issue of sensitivity checks of critical infrastructure objects from both scientific and practical perspectives; identifying the main types of emergency entities' hazards relevant during armed conflict; determining key criteria and indicators of CIO susceptibility; developing a methodological approach to vulnerability assessment incorporating comprehensive risk analysis; examining opportunities to integrate modern technologies (Geographic Information Systems, artificial intelligence, early detection systems, etc.) into fragility estimation and monitoring processes; and providing recommendations to improve resilience and protection of crucial assets at the national level.

**Summary of the main material.** Vulnerability assessment of critical infrastructure facilities involves identifying, analyzing, and prioritizing weaknesses within physical and cyber components of infrastructure, considering intersystem relationships that adversaries could exploit to disable or destroy emergency assets. That process encompasses CIO identification, risk review and assessment, and determining the probability and impact of threats on the given object. It also involves examining physical, technical, cybernetic, organizational, and human security factors.

The initial step in identifying critical facilities involves defining which specific entities constitute pivotal infrastructure. Examples may include energy systems (power plants, substations, pipelines), transportation nodes (bridges, railway stations, airports), communication and telecommunications networks, water supply and sewage systems, medical institutions, government buildings, and information centers, etc. Identification of CIOs is one of the essential stages in establishing an effective protection system and conducting vulnerability evaluation. Determining these objects facilitates resource prioritization, concentration of efforts on the most significant elements, and targeted planning of security measures.

According to the Law [7], critical infrastructure includes both physical and virtual system elements crucial for national security, economy, healthcare, environment, and public life. The above comprises energy facilities, transport, communication, IT systems, healthcare institutions, water supply, financial establishments, and others.

Identification of critical infrastructure objects must rely on established significance criteria, such as the scale of potential consequences when being disabled; the degree of dependency of other items or systems on their functionality; rapid recovery capability; and importance for national defense and safety.

Modern practice employs the following approaches to the identification of CIO [8]:

– sectoral analysis, which entails evaluating facilities within specific domains (e.g., energy, transportation, healthcare);

– matrix-based approach, focused on checking interdependencies among entities and the potential for cascading effects;

– information-analytical attitude, which involves processing large volumes of infrastructure-related data using Geographic Information Systems (GIS) technologies and decision-support tools;

– integrated risk-oriented practice, accounting simultaneously for threat levels, vulnerabilities, and potential consequences.

Within the European Union (EU), the European Programme for Critical Infrastructure Protection (EPCIP) system mandates the identification of European Critical Infrastructures (ECI) based on agreed standards. In the United States, identification is conducted across 16 pivotal infrastructure sectors under the National Infrastructure Protection Plan (NIPP). Both frameworks emphasize the priority of identifying dependencies and weak points in cross-sectoral interactions.

In wartime conditions, the identification process is complicated by several factors: limited access to current data due to security concerns; ongoing changes in infrastructure configuration due to destruction and relocation; the presence of hidden or non-standard assets playing a critical role; deficiencies in methodologies; and the absence of a unified state informational platform.

To enhance the effectiveness of CIO identification in Ukraine, standardized significance assessment criteria have been introduced. In addition, an integrated national information system for identification and monitoring has been developed [9, 10].

Successful identification of critical infrastructure requires a comprehensive approach that incorporates national legislation, international practices, risk-based methodologies, interdependencies among assets, and the deployment of advanced information-analytical tools. This task becomes particularly crucial in wartime conditions, where crucial infrastructure not only ensures societal functioning but also directly impacts national defense capabilities.

A comprehensive assessment of CIO vulnerability [1, 11] is unattainable without an in-depth analysis of potential threats. At this stage, threat sources, their nature, possible development scenarios, impact levels on the entities, and likelihood of occurrence must be identified. All threats may conventionally be classified into three primary categories: natural, technogenic, and anthropogenic.

Natural and technogenic threats [12, 13], although not the result of deliberate human action, can inflict significant damage on critical infrastructure, causing large-scale disruptions in its functionality. Anthropogenic threats stem from intentional or unintentional human activity.

Natural hazards encompass phenomena resulting from environmental processes independent of human activity. Earthquakes, for example, pose a significant risk to strategically important facilities – especially in seismically active regions – including vulnerable engineering structures, pipelines, power plants, and bridges. Floods threaten sites located near rivers, bodies of water, or low-lying areas. Disruptions in water supply, sewage systems, or electricity networks can lead to large-scale humanitarian and ecological consequences. Fires (particularly wildfires) may damage power grids, telecommunication towers, and logistics hubs. In the context of climate change, the increasing frequency and intensity of natural disasters necessitate the inclusion of new risk factors in monitoring and response systems.

Technogenic dangers stem from malfunctions, failures, or accidents due to the technical condition of facilities or human error. Industrial incidents (e.g., at chemical plants or nuclear power stations) may cause cascading effects across interconnected infrastructure elements. Disruptions in energy supply systems or information networks impair critical services (communications, healthcare, and public safety). Explosions, gas leaks, and structural collapses often result from equipment wear, non-compliance with safety protocols, or material fatigue. A particular characteristic of man-made threats is their potential for cumulative escalation – minor failures in one subsystem can provoke widespread breakdowns in others.

The next category of threats exposed to the CIO comprises anthropogenic threats. This is the most dangerous and dynamic group, arising from intentional or unintentional human activity. Under current wartime conditions, such dangers are particularly relevant for Ukraine. These include terrorist acts aimed at destabilization, spreading panic, and damaging vital infrastructure (e.g., water supply systems, communication nodes, and power stations); military assaults, including missile strikes, shelling, seizure of strategic points, and sabotage (with energy transport systems, bridges, airports, and logistics centers being especially at risk); and cyberattacks (targeting IT infrastructure, control systems hits (SCADA), databases, and communication channels). Threats posed by UAVs used by the enemy for reconnaissance or direct attacks on CIOs (substations, oil depots, warehouses, and air defense facilities) are becoming increasingly acute.

All anthropogenic risks are marked by high unpredictability, rapid execution, and the capacity to inflict substantial social, economic, and security damage.

Threat analysis enables not only the identification of potentially harmful impacts on CIOs but also the development of appropriate protection and response scenarios. In the context of hybrid warfare, priority must be given to addressing anthropogenic hazards, particularly those posed by advanced attack vectors – cyber tools and UAVs. Nevertheless, natural and technogenic factors should not be overlooked, as they often trigger sequential failures in complex infrastructure networks. The principal criteria and indicators used to assess the protection status of critical infrastructure objects are outlined in Order [2].

Vulnerability assessment becomes crucially important for effective planning of protective measures and enhancing the resilience of CIOs. It enables the determination of an object's ability to withstand external impacts, promptly identify threats, and mitigate the consequences of disasters. This process should be based on an integrated approach that considers technical, organizational, personnel-related, and technological aspects.

The first essential factor is the evaluation of the facility's physical condition and the presence of engineering barriers capable of preventing threats or reducing their effects. This includes assessing the degree of wear and tear of buildings, engineering systems, supporting structures, defensive fortifications, and the presence of impact-resistant, fire-resistant, or sealed components. It is also important to consider the adaptability of infrastructure to possible changes, including the ability to withstand shockwaves or power outages.

Another important aspect is the level of security and physical protection of CIOs. This encompasses the organization of facility practical security, the presence of surveillance posts, access control points, perimeter defense, access control, and alarm systems. The interaction between the security services of the object and the Security and Defense Forces of Ukraine [14] is also analyzed. Protecting critical infrastructure sites requires a holistic approach and coordinated cooperation among all components of Ukraine's security and defense sector. The entities comprising the National System for Critical Infrastructure Protection include:

– the Armed Forces of Ukraine (AFU);
– the Security Service of Ukraine (SSU);
– the National Guard of Ukraine (NGU) [15];
– the National Police of Ukraine (NPU);
– the State Emergency Service of Ukraine (SESU);
– the State Border Guard Service of Ukraine (SBGSU);
– local government authorities;
– private sector and critical infrastructure operators;
– international partners, allies, and others.

The effective safeguarding of CIOs depends on an established communication mechanism, joint threat assessment, information sharing, and coordinated response. The Armed Forces of Ukraine serve as the primary defense entity tasked with protecting strategically important installations, military bases, and state institutions from aerial threats.

To enhance the quality of preparedness, strategic development and training activities are actively pursued, including:

– joint exercises with NATO ally countries aimed at improving tactics for protecting and defending critical infrastructure facilities (CIOs);
– development and implementation of cutting-edge technologies and tactical solutions.

The coordinated efforts of the Security Service of Ukraine (SSU), National Guard of Ukraine (NGU), National Police of Ukraine (NPU), and the State Emergency Service of Ukraine (SESU) are essential components of critical infrastructure security. Effective protection must serve not only a passive but also an active role – it should empower swift response to breaches or emerging threats [16].

A significant reduction in vulnerability is achieved through the deployment of advanced threat detection systems: both physical (video surveillance, sensor networks, security detectors) and cyber (network monitoring tools, IDS/IPS, behavioral analysis platforms). Integrated response systems play a crucial role, as they can autonomously detect and categorize threats, initiate security protocols, or alert relevant emergency services.

The level of staff qualification and readiness to respond to emergencies at CIOs represents one of the most decisive vulnerability assessment criteria. The human factor is critically important in ensuring the security of essential infrastructure. Personnel preparedness, familiarity with crisis-response protocols, and participation in regular drills and simulations directly affect the employee's ability to respond promptly to potential hazards. This includes the availability of evacuation plans, emergency mitigation procedures presence, and affordability of personal protective equipment and medical support.

Vulnerability assessments for CIOs must be conducted systematically and from a multidisciplinary perspective. Even a single deficiency across any of the listed factors significantly increases the likelihood of operational failure or destruction. Thus, effective sensitivity management requires more than technical solutions. It also demands organizational maturity, interagency collaboration, and continuous modernization of security systems in line with evolving threat landscapes [17, 18].

An essential area of focus in the vulnerability evaluation of frail entities is the assessment of potential impact in the event of a successful strike. Estimating the consequences of an attack on the CIO is an integral part of risk analysis and long-term security planning. This stage involves determining the scope and depth of both direct and indirect effects of the incident on civilian life, economic performance, interdependent systems, and the broader socio-political stability of the region and the state as a whole.

Damage to critical infrastructure can produce immediate and cascading consequences for public health, safety, and the quality of life of the citizens. For instance, the disruption of energy assets may lead to the following: power outages affecting residential districts, hospitals, and heating systems in winter; destruction of water supply or wastewater systems that poses sanitary and epidemiological hazards; impairment of transport framework complicates evacuation, delivery of humanitarian aid, and emergency services; stress and panic among civilians in the context of prolonged resource shortages can incite increase of social tensions, and trigger civil unrest.

The economic repercussions of infrastructure damage can be enormous. These consequences include: direct losses – costs associated with rebuilding destroyed facilities, compensating for damages, and implementing temporary security measures; indirect losses – production halts, reduced transportation volumes, job losses, and declines in tax revenue; and long-term economic impacts – diminished investment appeal of the region, disruption of supply chains, and depreciation of strategic assets (such as losses in the agricultural sector due to the lack of access to irrigation or electricity). Such damages may occur at both regional and national scales.

The disruption of interconnected facilities or systems has a critical effect on the overall resilience and operational stability of the primary asset. In the process of vulnerability assessment, intersystem dependencies demand particular attention. Critical infrastructure constitutes a complex, interdependent network in which the failure of a single component may trigger cascading breakdowns in others. For instance, the disabling of a power substation may halt the operation of water utilities, hospitals, or transportation networks. Likewise, an attack on a communication hub could paralyze emergency alert and coordination systems. On top of that, incapacitation of a railway junction might obstruct the delivery of energy supplies to other regions.

Social and political destabilization significantly influences the security environment surrounding an asset. That is why its potential consequences must be factored into vulnerability assessments. The ramifications of infrastructure disruption often go beyond physical or material losses, extending into the realm of societal and political stability. Potential outcomes include loss of public trust in government institutions if they are perceived as unable to prevent or respond effectively to a crisis; heightened panic, protest movements, and the amplification of hostile information campaigns; exploitation of incidents by internal or external actors for political manipulation or to escalate tensions; and violations of Ukraine's international obligations. This is especially relevant for strategically significant facilities – such as hospitals, government buildings, or energy installations – whose destruction generates widespread public concern.

Impact assessment not only helps estimate the scope of potential damage but also enables the prioritization of CIO protection. Security plans and emergency response strategies must assign special attention to bodies whose disruption could simultaneously affect multiple domains – humanitarian, economic, and social. This analysis lays the groundwork for crisis management planning and the efficient allocation of resources during emergencies.

Therefore, the assessment of critical infrastructure vulnerability is a fundamental instrument for strengthening resilience, ensuring timely threat response, and minimizing the consequences of emergencies.

Evaluating CIO susceptibility involves the application of various methodologies [19, 20] that facilitate comprehensive risk analysis and the projection of their potential impact on safety. Multiple approaches to such assessments exist, which can be generally categorized as quantitative, qualitative, or integrated methods.

Quantitative methods provide objective numerical indicators of risks and the likelihood of damage. Therefore, they are essential for making informed decisions regarding the protection of the CIO. That approach relies on mathematical modeling, probabilistic analysis, and scenario simulation. It enables the quantification of an asset's risk or vulnerability level, as well as the assessment of the effectiveness of protective measures. The most widely used quantitative techniques are listed below.

1. Probabilistic Risk Assessment (PRA) – enables consideration of all possible development scenarios and determines the likelihood of each one.

2. Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) – used to identify critical failure points and failure chains.

3. Multi-criteria optimization methods – allow for the simultaneous evaluation of multiple impact factors (e.g., security status, system reliability, logistical connections, etc.).

4. Scenario-based impact modeling – applied to forecast the consequences of various threats.

Qualitative methods are based on expert evaluation, analytical observations, and descriptive analysis. These approaches are useful for addressing complex, insufficiently formalized factors affecting CIO vulnerability. Qualitative assessments of the points of failure rely on expert judgment, contextual analysis, and structured information-gathering techniques. They are particularly valuable when data availability is insufficient for mathematical modeling. The principal qualitative methods include the standing under items.

1. SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) facilitates the identification of internal strengths and weaknesses, external threats, and opportunities for protection.

2. The DELPHI method involves multi-round expert surveys to reach consensus in evaluations.

3. Structured interviews and surveys are used to gather insights from operations, safety, and CIO management professionals.

4. Analytic Hierarchy Process (AHP) allows the decomposition of complex decisions and the evaluation of vulnerability across several parameters.

Integrated methods combine elements of both quantitative and qualitative analysis. They offer a more comprehensive and balanced assessment of sensitivity by merging precise data with expert insight. In contemporary practice, integrated vulnerability assessment methods uniting quantity and quality vision are considered the most effective as they:

– provide a more holistic view of an asset's susceptibility by incorporating both objective measurements and subjective evaluations;

– increase result reliability by reducing errors typically inherent in any single approach;

– allow adaptation to diverse types of infrastructure and threat profiles.

Integrated approaches are often implemented in the form of models that fuse multiple data sources and analytical techniques. These may take the shape of GIS-based systems, information-analytical platforms, or digital twins of groundwork assets, enabling continuous data updates and real-time vulnerability monitoring.

The analysis of sensitivity assessment methods is a pivotal component in developing a comprehensive security strategy. That is because it enables not only the identification of potential hazards to facilities but also the planning of effective countermeasures.

Examples of vulnerabilities under martial law illustrate how external threats can significantly disrupt the functioning of CIOs, emphasizing the urgency of adopting a systematic approach to their assessment and protection. The full-scale military invasion of Ukraine, launched in 2022, drastically altered existing strategies for safeguarding critical infrastructure. The hostilities – characterized by targeted, systematic attacks on CIOs – have revealed their heightened exposure to a wide range of threats (from physical destruction to informational interference).

Since 2022, the russian federation has carried out numerous large-scale missile and drone strikes against Ukraine's energy infrastructure. The objective of these assaults was to incapacitate essential components of the national power system. These include thermal power plants (TPPs), high-voltage substations, transformer stations, and generation and dispatch facilities. As a result, millions of Ukrainians were subjected to prolonged cuts in electricity, heating, and water supply. These attacks revealed the significant susceptibility of the energy sector to precision missile strikes and kamikaze drones, as well as the limited availability of backup capacities within the power grid.

Damage to transportation infrastructure amid armed conflict leads to disruptions in logistical chains, restricts the mobility of defense forces, and complicates evacuation and humanitarian operations, making it one of the most vulnerable components of the critical framework. Rail junctions, bridges, and logistics hubs have repeatedly been the aims of missile strike launches. For example, corruption of railway tracks in the Dnipropetrovsk, Kyiv, and Lviv regions caused delays in cargo transportation. The destruction of bridges and rail crossings in frontline areas hampered the evacuation of civilians and the delivery of ammunition. A missile strike on the train station in Kramatorsk in April 2022 resulted in numerous civilian casualties. Described cases underscore the high susceptibility of transport infrastructure to precision weaponry and highlight the severe humanitarian and military consequences of such attacks.

Cyberattacks on digital infrastructure during martial law [21] can lead to communication breakdowns, loss of access to critical data, and failures in energy, financial, and administrative systems, making it a key vulnerability zone in today's pivotal root landscape.

In addition to physical strikes, cyber operations against both state and private information systems intensified significantly between 2022 and 2025. Notable examples include attacks on government portals and databases (such as the "Diia" platform and national registries); breaches of banking systems and disruptions to payment infrastructure; and DDoS attacks on telecommunications companies that hindered communication and coordination during emergencies. These incidents reveal a critical dependence of administrative and financial institutions on digital services and expose the absence of a robust digital cyber-reserve infrastructure.

The examples presented above illustrate that, under conditions of war, critical infrastructure assets become systematic targets of enemy operations. And their destruction or incapacitation results in widespread social, economic, and humanitarian fallout. Traditional approaches to CIO protection must be re-evaluated, and there is a pressing need to implement advanced monitoring technologies, countermeasures, and recovery systems, as well as to integrate security components into the state's strategic planning framework.

## Conclusions

In summary, vulnerability assessment constitutes a crucially important element of safeguarding critical infrastructure facilities, particularly under wartime conditions. Conducting such estimations enables the identification of the most exposed infrastructure components; supports the development of well-founded plans for the modernization and fortification of the entities; helps determine priority areas for investment in protective technologies; and facilitates the creation of effective response and recovery scenarios in the event of emergencies.

Amidst persistent threats posed by modern warfare technologies, Ukraine must strengthen its own system of sensitivity assessment and monitoring. This includes the implementation of integrated investigative models that combine both quantitative and qualitative approaches; the deployment of early warning systems and automated risk analysis tools; the advancement of interagency coordination in the field of critical infrastructure protection; and the incorporation of international experience and standards.

A comprehensive and systematic vulnerability assessment must serve as the foundation for shaping a national pivotal infrastructure security strategy. It should be capable of reinforcing overall state resilience and withstanding the complex dangers of modern hybrid warfare.

A direction for further research involves the examination of global practices in countering threats to critical infrastructure objects, the incorporation of international expertise, and the adaptation of global standards to the Ukrainian context.

## References

1. *Nakaz Derzhavnoho komitetu yadernoho rehuliuvannia Ukrainy "Pro zatverdzhennia Poriadku provedennia otsinky vrazlyvosti yadernykh ustanovok ta yadernykh materialiv" № 169* [Order of the State Committee for Nuclear Regulation of Ukraine "On approval of the Procedure for carrying out the assessment of the vulnerability of nuclear facilities and nuclear materials" activity no.169]. (2010, November 30). Retrieved from: https://surl.li/ulwcqv (accessed 7 April 2025) [in Ukrainian].

2. *Nakaz Administratsii Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy "Pro zatverdzhennia Metodyky ta Kryteriiv i pokaznykiv otsinky stanu zakhyshchenosti obiektiv krytychnoi infrastruktury" № 17* [Order of the Administration of the State Service for Special Communications and Information Security of Ukraine "On Approval of the Methodology and Criteria and Indicators for Estimating the Status of Security of Indoor Infrastructure Objects" activity no. 17]. (2025, January 14). Retrieved from: https://surl.lu/vyxbiv (accessed 7 April 2025) [in Ukrainian].

3. Bobro D. H. (2015). *Vyznachennia kryteriiv otsinky ta zahrozy krytychnii infrastrukturi* [Definition of criteria for the assessment of threats to indoor infrastructure]. *Stratehichni priorytety. Seriia: ekonomika*, no. 4 (37), pp. 83–93. Retrieved from: https://surl.li/prjzyq (accessed 7 April 2025) [in Ukrainian].

4. Kaplia I. V., Tertyshnyi B. V. (2024). *Metodyka otsiniuvannia zahroz obiektam krytychnoi infrastruktury pid chas vohnevoho vplyvu protyvnyka* [Methodology for assessing threats to indoor infrastructure facilities during the enemy's fire impact]. *Social Development and Security*, no. 5 (14), pp. 215–221. DOI: https://doi.org/10.33445/sds.2024.14.5.21 [in Ukrainian].

5. Murasov R. K., Nikitin A. V., Meshcheriakov I. V., Pidhorodetskyi M. O., Poplavets S. I. (2023). *Metodyka otsiniuvannia zahroz i ryzykiv dlia obiektiv krytychnoi infrastruktury za stsenariiamy rozvytku nadzvychainykh sytuatsii* [Methodology for assessing threats and risks for critical infrastructure objects under

emergency development scenarios]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony,* no. 3 (48), pp. 35–43. DOI: https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [in Ukrainian].

6. Murasov R. K., Melnyk Ya. V. (2023). *Otsiniuvannia zakhyshchenosti kiberprostoru obiektiv krytychnoi infrastruktury Ukrainy* [Assessment of the congestion of cyberspace by the objectives of Ukraine's infrastructure]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, no. 1 (46), pp. 41–44. DOI: https://doi.org/ 10.33099/2311-7249/2023-46-1-41-44 [in Ukrainian].

7. *Zakon Ukrainy «Pro krytychnu infrastrukturu» № 1882-IX* [Law of Ukraine about Indoor Infrastructure activity no. 1882-IX]. (2021, November 16). *Vidomosti Verkhovnoi Rady Ukrainy*, no. 5, art. 13. Retrieved from: https://zakon.rada.gov.ua/laws/show/1882-20#Text (accessed 7 April 2025) [in Ukrainian].

8. Toliupa S., Parkhomenko I., Antonyuk V. (2021). Method for Identification of Critical Information Infrastructure Objects of the State. In: Proceedings of the 1st International Workshop on Cyber Hygiene – CyberHygiene 2021. *CEUR Workshop* Proceedings, vol. 3179, pp. 262–271 [in English].

9. *Nakaz Administratsii Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy "Pro zatverdzhennia Metodychnykh rekomendatsii shchodo katehoryzatsii obiektiv krytychnoi infrastruktury" № 23* [Order of the Administration of the State Service for Special Communications and Information Security of Ukraine "For approval of methodological recommendations for the categorization of indoor infrastructure facilities" activity no. 23]. (2021, January 15). Retrieved from: https://surli.cc/kznhgg (accessed 7 April 2025) [in Ukrainian].

10. *Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia Poriadku vedennia Reiestru obiektiv krytychnoi infrastruktury, vkliuchennia takykh obiektiv do Reiestru, dostupu ta nadannia informatsii z noho" № 415* [Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for maintaining the Register of indoor infrastructure facilities, including such facilities in the Register, and access to and provision of information from it" activity no. 415]. (2023, April 28). Retrieved from: https://surl.li/lmhjfw (accessed 7 April 2025) [in Ukrainian].

11. *Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia Poriadku provedennia monitorynhu rivnia bezpeky obiektiv krytychnoi infrastruktury" № 821* [Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for monitoring the level of security of indoor infrastructure facilities" activity no. 821]. (2022, July 22). Retrieved from: https://surl.li/qgwnjm (accessed 7 April 2025) [in Ukrainian].

12. Onopriienko O. S., Sporyshev K. O. (2018). *Zmist zavdan syl Natsionalnoi hvardii Ukrainy pry vynyknenni nadzvychainoi sytuatsii vnaslidok avarii na hidrotekhnichnykh sporudakh* [The task force of the National Guard of Ukraine in the event of an emergency situation resulting from an accident on hydrotechnical structures]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, no. 5, pp. 243 – 247 [in Ukrainian].

13. Herasymenko O. M. (2024). *Zahrozy obiektam krytychnoi infrastruktury Ukrainy v umovakh voiennoho stanu* [Threats to indoor infrastructure facilities of Ukraine under martial law]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: pravo*, vol. 3 (84), pp. 257–263 [in Ukrainian].

14. Nazarenko O. L., Godlevskyi S. O., Danko V. V., Fedorenko V. O. (2025). Protecting Ukraine's critical infrastructure from drone threats: The role of security and defence forces. Actual Issues of Modern Science. *European Scientific e-Journal*, 37. Ostrava. Retrieved from: https://eiid.eu/ftpgetfile.php?id=248 (accessed 17 April 2025) [in English].

15. Nazarenko O. L. (2025). *Osoblyvosti okhorony obiektiv krytychnoi infrastruktury pidrozdilamy Natsionalnoi hvardii Ukrainy* [Features of the protection of indoor infrastructure facilities are provided by the National Guard of Ukraine]. Proceedings of the 2th International scientificand practical conference *"Aktualni problemy diialnosti skladovykh sektoru bezpeky i oborony Ukrainy v umovakh osoblyvykh pravovykh rezhymiv: potochnyi stan ta shliakhy vyrishennia"* (Ukraina, Kharkiv, March 20, 2025). Kharkiv : NA NHU, pp. 370–371 [in Ukrainian].

16. Yaremenko O. I., Strakhnitskyi Ya. O. (2022). *Vyznachennia ta upravlinnia zahrozamy u strukturi derzhavnoi polityky zakhystu krytychnoi infrastruktury* [The designation of this administration poses a threat to the structure of state policy on the protection of critical infrastructure]. *Universytetski naukovi zapysky*, vol. 3 (87), pp. 73–82. DOI: DOI: https://doi.org/10.37491/UNZ.87.6 [in Ukrainian].

17. Shaptala S. O., Romanenko Ye. O., Khrashchevskyi R. V. (2023). *Vykorystannia lazeriv dlia protydii bezpilotnym litalnym aparatam* [Using lasers to protect unmanned aerial vehicles]. *Nauka i tekhnika sohodni. Seriia: tekhnika*, no. 11 (25), pp. 617 – 629. Retrieved from: https://surl.li/ejtqpz (accessed 17 April 2025) [in Ukrainian].

18. Shumyhai O. V., Yermolenko O. V. (2020). *Suchasnyi stan bahatofunktsionalnykh zasobiv ta kompleksiv radioelektronnoi borotby* [Current state of multifunctional devices and complexes of radio-electronic warfare]. *Zbirnyk naukovykh prats Derzhavnoho naukovo-doslidnoho instytutu vyprobuvan i sertyfikatsii ozbroiennia ta viiskovoi tekhniky,* vol. 3 (5), pp. 119–125. DOI: https://doi.org/10.37701/dndivsovt.5.2020.14 [in Ukrainian].

19. Murasov R., Melnyk Ya., Marko V. (2022). *Porivniannia isnuiuchykh metodyk otsiniuvannia zahroz i ryzykiv dlia potentsiino-nebezpechnykh obiektiv krytychnoi infrastruktury v zoni vedennia boiovykh dii* [Comparison of existing methods for assessing threats and risks for potentially dangerous objects of indoor infrastructure in the zone of conducting combat operations]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony,* no. 3 (45), pp. 32–36. DOI: https://doi.org/10.33099/2311-7249/2022-45-3-32-36 [in Ukrainian].

20. Ozkan C., Singelee D. (2024). Evidence-Based Threat Modeling for ICS // arXiv preprint arXiv:2411.19759. Retrieved from: https://arxiv.org/abs/2411.19759 (accessed 17 April 2025) [in English].

21. Kovalchuk V. V., Sydorenko I. M. (2024). *Systema kiberzakhystu obiektiv krytychnoi infrastruktury v umovakh viiny* [Cybersecurity system for indoor infrastructure facilities in the conditions of the virus]. *Naukovyi visnyk KINHU,* vol. 2, pp. 43–48. DOI: https://doi.org/10.59226/2786-6920.2.2024.43-48 [in Ukrainian].

*The article was submitted to the editorial office on 5 June 2025*

**УДК 351.865**

**О. Л. Назаренко, О. М. Головань, В. В. Рудинський**

## ЩОДО ПИТАННЯ ОЦІНЮВАННЯ ВРАЗЛИВОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

*У сучасних умовах, особливо у воєнний час, питання захисту об'єктів критичної інфраструктури в Україні набуває першочергового значення. Оцінювання вразливості таких об'єктів дає змогу виявити слабкі місця в системі безпеки, запобігти потенційним атакам і забезпечити ефективне планування заходів реагування у межах забезпечення державної безпеки.*

*Актуальність цього питання зумовлює вдосконалення комплексної методології оцінювання вразливості об'єктів критичної інфраструктури, яка була б адаптованою до умов воєнного стану. Наявні підходи є фрагментарними і дещо застарілими, оскільки розроблені в контексті мирного часу. Крім того, практична реалізація заходів із захисту інфраструктури часто не має системного характеру, що може негативно позначатися на загальному рівні національної безпеки.*

*Отже, оцінювання вразливості критичної інфраструктури потребує науково обґрунтованого підходу, який би враховував специфіку сучасних воєнних загроз, використовував міждисциплінарні методи аналізу й був підґрунтям для ухвалення рішень у сфері державної безпеки. У нинішніх умовах оцінювання вразливості критичної інфраструктури набуває особливої актуальності.*

*Оцінювання вразливості об'єктів критичної інфраструктури передбачає аналіз їхньої безпеки та фізичної захищеності (заходи фізичного захисту, системи контролю доступу, спостереження та сигналізації), а також ефективну взаємодію сил охорони об'єкта із суб'єктами Національної системи захисту критичної інфраструктури України, зокрема Збройними Силами України, Службою безпеки України, Національною гвардією України, Національною поліцією України, Державною службою з надзвичайних ситуацій, Державною прикордонною службою України, органами місцевого самоврядування та іншими відповідними суб'єктами.*

*Досліджено питання оцінювання рівня вразливості об'єктів критичної інфраструктури та сформовано системний і багатовимірний підхід до аналізу загроз. Проаналізовано можливі наслідки* *пошкодження об'єктів критичної інфраструктури для населення, зокрема ризики соціальної та політичної дестабілізації.*

*Наведено методи оцінювання вразливості об'єктів критичної інфраструктури, а також приклади їх вразливості у воєнний час. Розглянуто результати міжнародної практики та здійснено аналіз потенційних загроз об'єктам критичної інфраструктури.*

***Ключові слова:*** *об'єкти критичної інфраструктури, вразливості, ризики, загрози, кібербезпека.*

**NAZARENKO Oleh** – Candidate of Military Sciences, Associate Professor of the Department of State Security, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0001-7579-0658

**HOLOVAN Oleh** – Candidate of Military Sciences, Associate Professor Head of the Department of State Security, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-7290-8021

**RUDYNSKYI Vitalii** – Doctor of Philosophy, Head of the Department of Management of Military Intelligence Units and Special Operations Forces, Military Academy (Odessa)
https://orcid.org/0000-0003-2066-865X