UDC 351.86:338.49

A. Kovalchuk

CONCEPTUAL APPROACH TO DEFINING DIRECTIONS FOR MINIMIZING THE AGGRESSIVE INFLUENCE OF THE RUSSIAN FEDERATION ON UKRAINE'S ENERGY CRITICAL INFRASTRUCTURE OBJECTS

The problem of the lack of a systematic approach to assessing the threats and consequences of attacks on Ukraine's critical infrastructure is investigated. A new methodological approach to evaluating aggressive influence on critical infrastructure objects is proposed in the form of a generalized verbal model of the response of critical infrastructure systems to aggression on the example of energy objects. Two trends for minimizing the effects of aggressive influence on the critical infrastructure system are considered: adaptation of the system to the conditions of aggression and active influence on the means of aggression (direct fire impact). The proposals for overcoming the energy crisis are presented and the necessity of a comprehensive approach to ensuring the resilience of critical infrastructure is substantiated.

Keywords: *critical infrastructure objects, aggressive influence, energy crisis, critical infrastructure resilience, impact minimization.*

Statement of the problem. Russian aggression, characterized by constant missile and cyberattacks on Ukraine's critical infrastructure (CI), poses a severe threat to national security, economic stability, and the well-being of the population. Critical infrastructure, particularly energy, transportation, communication, and information systems, is highly vulnerable to targeted attacks that can lead to significant loss of life, economic damages, and disruption of societal functions.

There is an urgent need for a clear framework to determine the directions for minimizing the impact of the russian federation's (rf) aggressive actions on Ukraine's CI. The lack of a systematic approach to assessing threats and consequences of attacks on these assets complicates decision-making processes regarding their protection and recovery. Moreover, existing protection methods do not always account for emerging threats, such as cyberattacks and disinformation campaigns, which make the critical infrastructure system more susceptible. Addressing this issue will enhance Ukraine's resilience to rf's aggressive actions and strengthen national security overall.

Analysis of recent research and publications. To date, there is a substantial amount of research dedicated to various aspects of CI protection issues. In particular, the theoretical and methodological foundations for ensuring CI protection systems are covered in the works of D. H. Bobro [1, 2] and O. M. Sukhodolia [3]; the study of the state CI protection system in Ukraine has been addressed by M. F. Kryshtanovych, Ya. Ya. Pushak, M. I. Fleichuk and V. I. Franchuk [4]; analyses of foreign experiences are described by V. O. Yevsieiev [5], O. P. Yermenchuk [6, 7], and S. S. Telenyk [8]; organizational, technical, and tactical aspects of engineering protection systems for CI are examined in the works of M. V. Koval, V. V. Koval, V. I. Kotsiuruba, A. S. Bilyk [9]; and the problem of protecting CI from cyber attacks has been studied by researchers such as K. Cherevko and D. Pashniev [10].

At the same time, there is a need for a systematic approach to defining directions for minimizing aggressive impacts on CI, as well as for improving methods to ensure its stable functioning under constant threats.

The purpose of the article is to define a concept for minimizing the impact of the rf on critical infrastructure and to provide recommendations for its practical implementation.

Summary of the main material. According to paragraph 13 of Article 1 of the Law of Ukraine "On Critical Infrastructure" critical infrastructure

facilities are defined as a set of infrastructure objects essential to the economy, national security, and defence, whose disruption could harm vital national interests [11].

The Law (paragraph 4 of Article 9) defines essential functions and services, the disruption of which leads to adverse consequences for Ukraine's national security, including: governance and provision of critical public (administrative) services; energy supply (including heat supply); water supply and sanitation; food supply; healthcare; information services; electronic communications; financial services; transportation; defence and national security; public order, administration of justice, detention; civil protection of the population and territories, rescue services, and others [11].

Among the primary CI facilities targeted by the rf in Ukraine since the beginning of the full-scale invasion, the following can be highlighted:

1. Energy infrastructure facilities. The russian occupying forces (hereinafter referred to as ROF) have been conducting regular attacks on power plants, substations, heat-generating facilities, and power transmission lines, causing widespread disruptions in electricity supply. This has led to a large-scale energy crisis, especially during the winter season. The destruction or damage of power generation facilities, such as thermal power plants (hereinafter referred to as TPPs) and hydroelectric power plants (hereinafter referred to as HPPs), results in reduced production capacity and creates a significant shortage of energy resources.

2. Transport infrastructure facilities. ROF strike railway stations, bridges, roads, and airports, disrupting logistics chains, complicating the transportation of goods and military equipment, and hindering the evacuation of civilians from dangerous areas. Targeted attacks on bridges aim to disrupt the mobility of Ukraine's Defence Forces (hereinafter referred to as UDF) and civilian structures, making the supply of goods and military aid as challenging as possible.

3. Communication infrastructure facilities. ROF target communication facilities, including television towers, internet hubs, and mobile networks. This leads to disruptions in telecommunications networks, complicating the coordination of actions for both the UDF and civilian structures, especially the units of the State Emergency Service of Ukraine. Russia also conducts extensive cyberattacks on Ukrainian critical infrastructure aimed at disabling information systems, disorganising communications, and creating chaos.

4. Water supply and sanitation systems. ROF attacks on water intake and pumping stations result in disruptions to water supply in populated areas, creating a humanitarian crisis, especially in regions where access to water is critically important.

5. Healthcare system facilities. ROF target hospitals, clinics, and other medical institutions, which complicates the provision of medical care and worsens conditions for treating the injured and sick.

6. Oil and gas industry facilities. Damage to the oil and gas infrastructure is estimated at $3.3 billion. ROF have destroyed nearly all oil refineries in Ukraine and a significant portion of the infrastructure for storing oil and petroleum products [12].

7. Defence-industrial complex facilities.

8. Agro-industrial complex facilities.

Overall, russian attacks on Ukraine's CI have a comprehensive and devastating impact on the country, creating numerous challenges across various areas of life and exacerbating the humanitarian crisis.

The impact of the russian federation on Ukraine's CI can be assessed through its consequences, which include: an energy crisis, reduced economic activity, a humanitarian crisis, the threat of an environmental catastrophe, and a decrease in the national resilience of Ukrainian's.

The energy crisis in Ukraine, marked by blackouts and rolling power outages, is a direct result of attacks on critical infrastructure. As of May 2024, the Kyiv School of Economics (KSE Institute) estimates the direct damages and indirect financial losses to Ukraine's energy sector from the war at $56.2 billion [12].

The greatest damages concern power generation facilities ($8.5 billion) and main power transmission lines ($2.1 billion). During the full-scale invasion, over 18 GW of power generation capacity was captured, including Europe's largest nuclear power plant, the Zaporizhzhia NPP. Additionally, the Kakhovka and Dnipro HPPs, as well as the Zmiivska and Trypilska TPPs, were completely destroyed. Private thermal power plants such as Ladyzhynska, Burshtynska, Dobrotvirska, Kurakhivska, Kryvorizka, and Prydniprovska TPPs suffered extensive damage – over 80 %. Approximately half of the high-voltage substations were also affected [12].

The destruction of key facilities has complicated the provision of stable energy supply. The energy balancing system has become less reliable, causing significant challenges in meeting electricity demand, especially during peak loads. In the face of a deficit in domestic generation capacity, Ukraine has been compelled to increase electricity imports

from neighbouring countries, which has raised costs and increased dependency on external suppliers.

The military actions have highlighted the vulnerability of energy CI to external threats. The occupation and destruction of key power generation facilities, such as TPPs and HPPs, along with damaged oil refineries and transmission lines, underscore the insufficient protection of critical infrastructure elements against physical attacks. Protecting energy facilities goes beyond physical security alone. Ensuring resilience to disruptions and the capacity to rapidly restore power supply, even amid the destruction of individual facilities, is essential. This is a critical aspect for maintaining the functioning of governmental, industrial, and social systems during wartime. The restoration of damaged facilities based on the principle of "build back better" [12] will contribute to the enhanced security and resilience of energy infrastructure.

Reduction in Economic Activity. The instability of energy supply due to the destroyed infrastructure has led to a significant decline in economic activity in Ukraine. Many industrial enterprises have been forced to either halt operations entirely or operate under restrictions, which has negatively impacted the country's economy. This, in turn, has resulted in a substantial decrease in GDP.

The humanitarian crisis resulting from the destruction of infrastructure has forced many people to leave their homes, leading to a new wave of internally displaced persons. The destruction of transport infrastructure has caused serious disruptions in logistics, complicating the delivery of humanitarian aid to affected regions, deepening the crisis, and creating additional challenges for the impacted communities. Evacuation has become a necessity for those in dangerous areas or regions where basic living conditions cannot be ensured.

In Mykolaiv, with a population of approximately 494,400 as of 1 March 2015, water disappeared after ROF blew up a water pipeline in Kherson region. In Chernihiv, where the population was 294,100 at the beginning of 2016, water supply is provided from wells, and damage to the pumping station due to russian shelling led to a water cut-off in the city.

According to the Resolution of the Cabinet of Ministers of Ukraine dated 9 October 2020 No. 1109 (as amended on 16 January 2024 No. 48), the recovery time for the centralized drinking water supply service to operate normally for more than 145,000 residents should not exceed 24 hours, and the level of negative impact is assessed as having catastrophic consequences (4 points) [13].

The situation with water supply in cities such as Mykolaiv and Chernihiv has demonstrated the vulnerability of critical infrastructure elements during wartime. This raises the question: what should be prioritized for protection – the facilities themselves or their functions? Protecting the facilities involves minimizing risks, reducing their vulnerability, and lessening the consequences of potential damage. Conversely, when it comes to protecting functions, the main objective is to ensure their continuity and facilitate rapid recovery in the event of disruptions to the facilities [2].

Such cases indicate that, in addition to the physical protection of facilities, it is also essential to have contingency plans for the restoration of critical functions, as observed in the cases of ensuring water supply.

The threat of ecological catastrophe is a serious issue that has arisen as a result of the war. The destruction of industrial facilities and energy infrastructure has led to the release of harmful substances, negatively impacting the environment. Missile strikes and other military actions have also damaged natural resources, affecting forests, rivers, and other natural sites, further complicating the ecological situation. The explosion of the Kakhovka HPP by ROF stands out as a terrorist act with the most significant impact on natural ecosystems among all events that have occurred in Ukraine since 24 February 2022 [14]. Its consequences for wildlife, the economy, energy, the population, and, in general, for Ukraine's national security are catastrophic. One of the largest impacts of this disaster is on fish resources: Ukraine has lost a vast amount of fish stocks [14]. However, the effects on territories of the natural reserve fund, internationally significant conservation sites, river flooding, salinization, and pollution of the Black Sea remain under-researched.

The reduction of national resilience among Ukrainians is linked to the security and protection of CI, which includes: stable food supply, water supply, energy supply, and heating; cybersecurity; sustainable functioning of the transport system; security and uninterrupted operation of information services and communication services; provision of defence and law enforcement; and the ability of the healthcare system to function under increased stress. These elements are crucial components of Ukraine's national resilience system [15].

The destruction of CI has a significant impact on the national resilience of Ukraine, as it provides the basic necessities for the population, stability of state institutions, and the economy. The loss of access to

energy, water supply, and heating leaves millions of people without essential resources for survival, especially during the cold season. This leads to increased mortality, decreased morale in society, and serious social challenges. The shutdown of enterprises due to disruptions in the supply of electricity or other resources results in economic losses, rising unemployment, and a decline in the standard of living for the population. The constant threat of attacks on infrastructure intensifies feelings of danger, fear, and distrust in the government's ability to ensure the protection and safety of its citizens.

Thus, the destruction of critical infrastructure undermines Ukraine's national resilience, increasing its vulnerability to external and internal threats.

Adaptation of the CI system to external threats involves, first, assessing the current state of the system and the consequences of aggressive impacts, and second, identifying directions for minimizing the influence of external threats within the constraints inherent to this system.

Assessing the consequences of the aggressive influence of the rf on the CI system of Ukraine primarily involves determining an effectiveness indicator for this system $Q(u)$, which depends on the state u of the country's CI.

The main requirement for selecting such an effectiveness indicator $Q(u)$ is its alignment with the system's goal, which is reflected in the desired (reference) outcome Y_0.

To evaluate the correspondence between the actual state of the system $Y(u)$ and the desired one Y_0, a numerical function must be introduced on the set of results u, representing a correspondence function defined as follows:

$$\rho = \rho[Y(u),\ Y_0], \qquad (1)$$

where *Y(u)* – represents the actual state of the system, encompassing the parameters u of CI;

Y_0 – denotes the desired (reference) state of the system.

The form of the correspondence function (1) depends on the specific goal of the system under investigation and the research task.

In general, the state of the system *Y(u)* can be treated as a random variable. Therefore, the correspondence function (1), as a numerical function of a random process, will also be random. If the outcome is expressed as a random variable, the distribution *Y(u)* depends on the parameters (strategies) u.

Thus, based on the concept of the correspondence function (1), an average value should be accepted as the criterion for the system's effectiveness $Q(u)$:

$$Q(u) = M\{\rho[Y(u), Y_0]\}, \qquad (2)$$

where $M\{*\}$ – operation of calculating the mathematical expectation for a random argument u.

If $Y(u)$ and Y_0 – are non-random variables, then the function (2) takes the following form

$$Q(u) = \rho[Y(u), Y_0].$$

The state's infrastructure Y_0 represents a multidimensional system that encompasses a finite set of local subsystems (structures) $Y_i(u) : Y_i(u) \in \Omega_Y,\ i \in [1, N]$; N – the total number of infrastructure elements.

In this case, to evaluate the effectiveness of a system of this class, it is necessary to use a vector indicator that combines the effectiveness indicators of the local subsystems of the infrastructure:

$$Q(u) = [Q_1(u), Q_2(u), \dots Q_i(u) \dots Q_N(u)], \qquad (3)$$

where $Q_i(u),\ i \in [1, N]$ – private characteristics of the result, which are determined in accordance with formula (2) and are equal to:

$$Q_i(u) = \mathrm{M}\left\{\rho\left[Y_i(u), Y_i^0\right]\right\}, i \in [1, N].$$

The transition to a vector efficiency indicator of the system (3) imposes additional requirements for the adequacy of the model of the system under study, with a minimal number of private indicators $Q_i(u), i \in [1, N]$.

The efficiency indicator of the system $Q(u)$ depends on the parameters (development strategies) of the objects u that are part of the critical infrastructure system.

It is determined over the set of allowable parameters (strategies) $\Omega_u : u \in \Omega_u$. In general, this dependency is defined by a mapping of the set of allowable parameters (development strategies) of the system Ω_u to the set of values of its effectiveness indicators:

$$F : \Omega_u \rightarrow Q(u).$$

Essentially, the display F corresponds to specific measures (strategies) for the development of critical

infrastructure and is defined in the form specified by a particular mathematical model of the system.

The conceptual result of the methodological approach to assessing aggressive impacts on CI is presented in Figure 1 as a generalized verbal model of the response of the CI system to the effects of aggressive means on the example of energy objects. According to this model, two trends for minimizing the consequences of aggressive impacts on the CI system are considered natural, namely:

1) adaptation of the CI system to conditions of aggression, here, it is important to highlight the priority of combining methods of parametric, structural, and alternative adaptation of the system;

2) active influence on external means of aggression through the use of firepower by the UDF, primarily focusing on their destruction.

The verbal model presented in Figure 1 is to some extent idealized. It is known that idealization is inherent in any model; however, this model (Figure 1) takes into account the key factors that determine the reaction (behaviour) of the CI system under conditions of external aggression and can be the subject of further research. The issue of integrating methods of parametric, structural, and alternative adaptation of the system is of particular interest.

The losses in Ukraine's energy sector due to the war are enormous and require a comprehensive approach to recovery. Moreover, the reconstruction process must not only restore what has been lost but also enhance resilience to future risks.

Considering these losses and the complicated provision of electricity to the population and CI, there is an urgent need for both immediate and strategic actions to restore stability and ensure the resilience of the energy system.

Resilience of critical infrastructure is the state of critical infrastructure in which its ability to operate in normal mode, adapt to constantly changing conditions, withstand threats, and quickly recover from any type of threat impact is ensured [11]. To overcome the energy crisis in this context, comprehensive measures are required, encompassing both short-term and long-term strategies. These include immediate infrastructure restoration, resource optimization, diversification of energy sources, infrastructure strengthening, international assistance, and long-term planning. Below are practical ways to adapt Ukraine's energy system to rf's aggressive impact on its critical infrastructure.

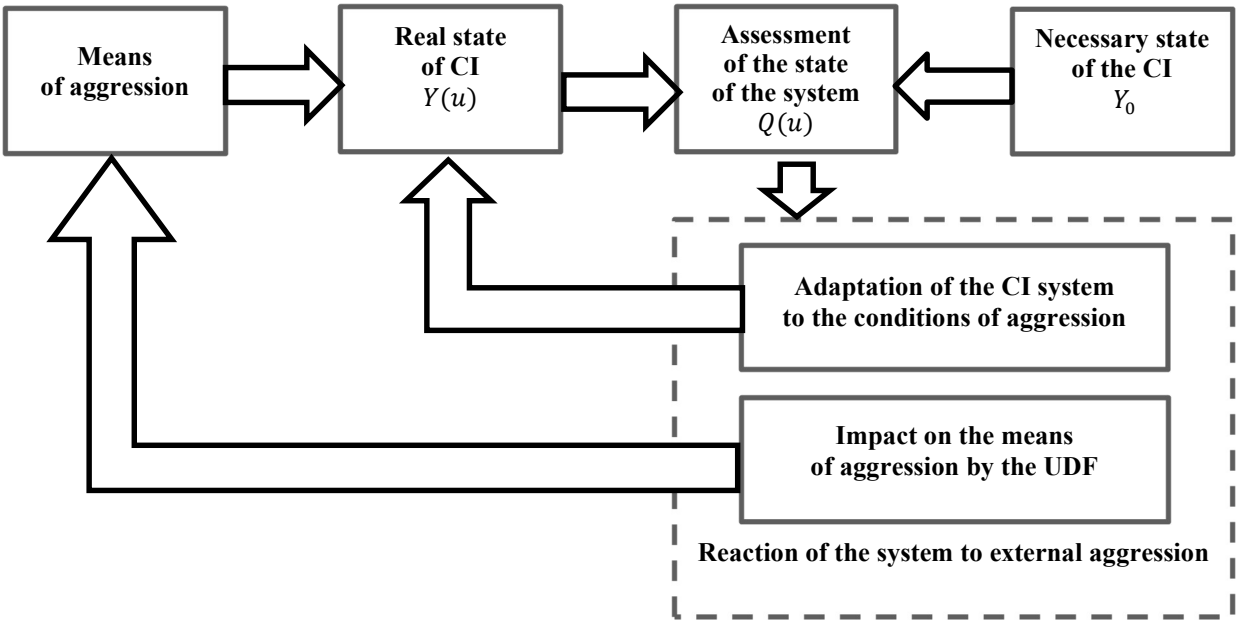

Figure 1 – Generalized verbal model of the CI system's response to the impact of external aggression means (on the example of energy objects)

Firstly, urgent measures must be taken to stabilize the system. This includes the rapid repair and restoration of damaged facilities, such as power plants and substations, along with the deployment of mobile generators to support critical infrastructure. In the event of a severe electricity shortage, Ukraine can increase imports from neighbouring countries. Rolling blackouts may also be part of the strategy to minimize adverse effects on the economy and society.

Secondly, it is essential to optimize energy resource use by implementing energy efficiency programs, modernizing buildings, and replacing inefficient equipment. Long-term solutions include diversifying energy sources, developing renewable sources, and, where feasible, expanding nuclear power. This approach will reduce dependence on traditional and vulnerable generation types.

Thirdly, energy infrastructure must be reinforced by protecting critical facilities and modernizing networks. Establishing air defence systems, decentralizing generation, and implementing smart grids for automatic power management can significantly improve system resilience.

Furthermore, it is advisable to develop international cooperation in the energy sector, as international assistance and coordination play a crucial role. Financial and technical support from international institutions, along with experience-sharing, can aid in the effective restoration and protection of the energy infrastructure.

Long-term development of Ukraine's energy sector must also be considered. This requires an energy security strategy, investments in scientific research, and new technologies, which will strengthen the resilience of Ukraine's energy system against future challenges.

To address the current energy crisis and ensure the energy system's resilience, Ukraine must implement a range of strategic measures. Infrastructure restoration, resource optimization, energy source diversification, infrastructure reinforcement, and international support are all essential elements for stabilizing the situation.

However, an effective solution to energy security also depends on the active involvement of the UDF, which play a critical role in safeguarding energy infrastructure and upholding national security amid russian air attacks. The UDF's actions in air defence, aviation and artillery support, cybersecurity, intelligence, and special operations, along with equipment modernization, are key to overcoming the energy crisis and ensuring the stability of the country's energy system.

The main ways in which the UDF can impact aggression means (Figure 1) to overcome the energy crisis include: 1) strengthening air defence (AD): deployment of AD systems around key energy facilities to protect against missile strikes, enhancing readiness to respond to threats; increasing the effectiveness of the early warning and missile alert system to enable timely AD activation and reduce consequences; 2) aviation and artillery support: detection and destruction of enemy missile launchers and transport vehicles from a distance to reduce the frequency and effectiveness of missile attacks; dismantling enemy logistics chains (ammunition depots, transport hubs, and other logistical facilities supporting missile strikes on Ukraine); 3) cybersecurity and information operations: ensuring the cybersecurity of energy facilities to prevent possible cyberattacks that could paralyze energy infrastructure operations or disrupt system management; identifying and neutralizing enemy information campaigns aimed at destabilizing the energy sector and inciting public panic; 4) intelligence and special operations: utilizing all available intelligence resources to locate enemy missile systems and plan operations to eliminate them; conducting special operations on the territory of the rf to destroy missile complexes that threaten Ukrainian infrastructure; 5) preparation and mobilization of reserves: conducting training and exercises for military personnel and rescue services to increase readiness for rapid response to new missile attacks and their consequences; deploying reserve forces to strengthen critical infrastructure protection, if necessary; 6) cooperation with international partners: obtaining additional AD assets (Patriot, IRIS-T, NASAMS), long-range missiles (ATACMS, Storm Shadow/SCALP or other precision missiles) to strike airfields, bases, and command centres from which missiles are launched, significantly enhancing UDF's ability to protect critical infrastructure; actively collaborating with partner intelligence services for timely information exchange on potential missile threats; 7) modernization of military equipment and armament: developing and procuring new weapons, military equipment, and technologies that can improve critical infrastructure protection efficiency, including unmanned aerial vehicles, electronic warfare systems, and anti-missile complexes; ensuring rapid repair and modernization of existing military equipment involved in protecting energy critical infrastructure.

Conclusions

To minimize the aggressive impact of the rf on Ukraine's CI, it is essential to implement a series of strategic and operational measures, considering two key trends: adapting the CI system to conditions of aggression and actively countering aggressive means (firepower impact).

Strengthening the protection of CI should involve bolstering a layered air defence system, modernizing air defence capabilities, and planning effective measures for their rapid restoration. Additionally, increasing capabilities to destroy missile carriers and launch complexes at their airfields and bases is essential to reduce the likelihood of successful attacks on these facilities.

Decentralization and redundancy are crucial for enhancing the resilience of infrastructure, especially in the energy sector. Transitioning to a more decentralized power generation system, including the development of renewable energy sources, can reduce vulnerability to attacks. Reserving critical assets, such as energy and water supply sources, is also an important step to ensure operational continuity if primary facilities are compromised.

Strengthening cybersecurity for information systems supporting infrastructure operations will help prevent cyberattacks that could paralyze control over these facilities. Regular exercises and testing of cybersecurity systems will ensure readiness to repel such attacks.

It is essential to enhance infrastructure resilience through engineering upgrades, introducing modern solutions for building reinforcement and CI protection. Implementing autonomous control systems will also enable facilities to operate independently of main networks in case of damage.

Expanding international cooperation is advisable to acquire advanced technologies and equipment for CI protection, as well as to facilitate intelligence sharing for timely threat response.

Rapid recovery and response to attacks on energy infrastructure are vital for national stability, especially given the ongoing regular attacks on Ukraine's energy facilities.

Ensuring public resilience through expanded information on threats and mitigation measures is also crucial.

Both long-term and short-term planning, along with investments in CI modernization, are necessary to strengthen its resilience. Developing security strategies and supporting modernization projects will help reduce vulnerabilities and ensure adequate protection.

Thus, implementing these measures will significantly reduce the aggressive impact of the rf on Ukraine's CI, requiring a comprehensive approach and resource allocation at the national, private, and international levels. This approach will help minimize the impact of attacks on the country's functioning and maintain resilience against persistent threats.

Further research will be aimed at identifying criteria and indicators for assessing the effectiveness of priority measures to minimize aggressive impact on Ukraine's CI.

References

1. Bobro D. H. (2015). *Vyznachennia kryteriiv otsinky ta zahrozy krytychnii infrastrukturi* [Determining criteria for evaluation and threats to critical infrastructure]. *Stratehichni priorytety*, no. 4, pp. 83–93 [in Ukrainian].

2. Bobro D. H. (2016). *Metodolohiia otsinky rivnia krytychnosti obiektiv krytychnoi infrastruktury* [Methodology for assessing the criticality level of critical infrastructure objects]. *Stratehichni priorytety*, no. 3, pp. 77–85 [in Ukrainian].

3. Sukhodolia O. M. (2020). *Derzhavna systema zakhystu krytychnoi infrastruktury v systemi zabezpechennia natsionalnoi bezpeky* [State system for critical infrastructure protection in the national security framework]. Kyiv : Natsionalnyi instytut stratehichnykh doslidzhen [in Ukrainian].

4. Kryshtanovych M. F., Pushak Ya. Ya., Fleichuk M. I., Franchuk V. I. (2020). *Derzhavna polityka zabezpechennia natsionalnoi bezpeky Ukrainy: osnovni napriamky ta osoblyvosti zdiisnennia* [State policy for ensuring Ukraine's National Security: main directions and implementation features]. Lviv : Spolom [in Ukrainian].

5. Yevsieiev V. O. (2016). *Mozhlyvi shliakhy udoskonalennia zakhystu krytychnoi infrastruktury Ukrainy z urakhuvanniam svitovoho dosvidu* [Possible ways to improve the protection of Ukraine's critical infrastructure taking into Account global experience]. *Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl imeni Ivana Kozheduba*, vol. 4, pp. 168–172 [in Ukrainian].

6. Yermenchuk O. P. (2017). *Normatyvno-pravove rehuliuvannia diialnosti u sferi zakhystu natsionalnoi krytychnoi infrastruktury: analiz ta uzahalnennia normotvorchoi praktyky SShA* [Normative and legal regulation of activities in the field of national critical infrastructure protection: analysis and generalization of legislative practices in the USA]. *Naukovyi visnyk Dnipropetrovskoho*

derzhavnoho universytetu vnutrishnikh sprav, vol. 3, pp. 135–140 [in Ukrainian].

7. Yermenchuk O. P. (2018). *Osnovni pidkhody do orhanizatsii zakhystu krytychnoi infrastruktury v krainakh Yevropy: dosvid dlia Ukrainy* [Main approaches to organizing critical infrastructure protection in european countries: experience for Ukraine]. Dnipro : Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav [in Ukrainian].

8. Telenyk S. S. (2018). *Dosvid pravovoho rehuliuvannia systemy zakhystu krytychnoi infrastruktury SShA* [Experience of legal Regulation of critical infrastructure protection system in the USA]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav,* vol. 2 (107), pp. 358–370 [in Ukrainian].

9. Koval M. V., Koval V. V., Kotsiuruba V. I., Bilyk A. S. (2022). *Orhanizatsiino-tekhnichni zasady pobudovy systemy inzhenernoho zakhystu obiektiv krytychnoi infrastruktury enerhetychnoi haluzi Ukrainy* [Organizational and technical principles of building the engineering protection system for critical infrastructure objects in Ukraine's Energy Sector]. *Nauka i oborona*, vol. 3-4, pp. 11–16 [in Ukrainian].

10. Cherevko K., Pashniev D. (2024). *Kiberataky na obiekty krytychnoi infrastruktury v umovakh vedennia viiny: kliuchovi poniattia* [Cyberattacks on critical infrastructure objects in the context of Warfare: key concepts]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy*, vol. 31 (1), pp. 209–219. DOI: https://doi.org/10.32631/vca.2024.1.15 [in Ukrainian].

11. *Zakon Ukrainy "Pro krytychnu infrastrukturu" № 1882-IX* [Law of Ukraine about critical infrastructure of Ukraine activity no. 1882-IX]. (2021, November 16). Retrieved from: https://zakon.rada.gov.ua/laws/show/1882-20#Text (accessed 10 September 2024) [in Ukrainian].

12. *KSE zbilshyla otsinku zbytkiv ta vtrat enerhosektoru Ukrainy do $56 mlrd* [KSE increased the estimate of losses and damages in Ukraine's energy sector to $56 billion. Ukrainian energy]. *Ukrainska enerhetyka*. Retrieved from: http://surl.li/cmettg (accessed 10 September 2024) [in Ukrainian].

13. *Postanova Kabinetu Ministriv Ukrainy "Deiaki pytannia obiektiv krytychnoi infrastruktury" № 1109* [Resolution of the cabinet of ministers of Ukraine "Some issues of critical infrastructure objects" activity no. 1109]. (2020, October 9). Retrieved from: http://surl.li/wdvycl (accessed 10 September 2024) [in Ukrainian].

14. Ukrainska pryrodookhoronna hrupa (2023). *Yakymy ye naslidky rosiiskoho teraktu na Kakhovskii HES dlia dykoi pryrody?* [The consequences of the russian terrorist attack on the Kakhovka Hydroelectric power station for wildlife?]. Retrieved from: http://surl.li/ffznsw (accessed 10 September 2024) [in Ukrainian].

15. Koval M. et al. (2023). *Theoretical and applied aspects of the Russian-Ukrainian war: hybrid aggression and national resilience*. Kharkiv : Technology Centre. PC. DOI: http://doi.org/10.15587/978-617-8360-00-9 [in English].

The article was submitted to the editorial office on 20.10.2024

УДК 351.86:338.49

А. Т. Ковальчук

КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ НАПРЯМІВ МІНІМІЗАЦІЇ АГРЕСИВНОГО ВПЛИВУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА ЕНЕРГЕТИЧНІ ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Досліджено проблему, пов'язану з тим, що бракує систематизованого підходу до оцінювання загроз і наслідків атак російської федерації на об'єкти критичної інфраструктури України. Визначено основні об'єкти критичної інфраструктури, які були уражені російськими окупаційними військами в Україні з початку повномасштабного вторгнення. Вплив росії на об'єкти критичної інфраструктури України розглянуто в контексті оцінювання його наслідків, серед яких виокремлено енергетичну кризу, зниження економічної активності, гуманітарну кризу, загрозу екологічної катастрофи, зниження національної стійкості українців.

Подано узагальнену вербальну модель реакції системи об'єктів критичної інфраструктури (на прикладі енергетичних об'єктів) на вплив засобів агресії як концептуальний результат методологічного підходу до оцінювання агресивного впливу на об'єкти критичної інфраструктури.

Запропоновано функцію відповідності, яка дає змогу оцінити відповідність реального стану системи об'єктів критичної інфраструктури еталонному. Розглянуто дві тенденції мінімізації наслідків агресивного впливу на систему об'єктів критичної інфраструктури: це адаптація системи до умов агресії та активний вплив Сил оборони України на зовнішні засоби агресії.

Викладено пропозиції щодо шляхів подолання енергетичної кризи, а саме: невідкладне відновлення інфраструктури, оптимізація використання ресурсів, диверсифікація джерел енергії, зміцнення інфраструктури, міжнародна допомога та довгострокове планування. Особливу увагу приділено значенню Сил оборони України у забезпеченні захисту енергетичної інфраструктури та підтримці національної безпеки в умовах проведення російською федерацією повітряних атак. Підкреслено необхідність комплексного підходу до забезпечення стійкості енергетичної системи та зменшення агресивного впливу на об'єкти критичної інфраструктури України із зосередженням зусиль на державному, приватному та міжнародному рівнях.

Ключові слова: *об'єкти критичної інфраструктури, агресивний вплив, енергетична криза, стійкість критичної інфраструктури, мінімізація впливу.*

Kovalchuk Andrii – Commandant of Military Academy (Odesa)
https://orcid.org/0009-0000-0907-6712