UDC 351.865

O. Nazarenko

S. Hodlevskyi

I. Skakalin

ORGANIZATION OF COMPREHENSIVE SECURITY MEASURES FOR CRITICAL INFRASTRUCTURE FACILITIES BY THE SECURITY AND DEFENSE FORCES OF UKRAINE

Key approaches to camouflage and equipping important state facilities and critical infrastructure facilities under martial law with engineering and engineering means are considered, taking into account the experience of their use by units of the Security and Defense Forces of Ukraine to ensure state security. Particular attention is paid to the principles of integration of natural and artificial elements of camouflage with engineering and technical means of protection, as well as the organization of security, taking into account the conduct of reconnaissance by the enemy in various ways and means to identify the locations of important state facilities and critical infrastructure facilities. Within the framework of the study, the problems of interaction between various components of the Security and Defense Forces of Ukraine in the process of protecting important state facilities and critical infrastructure facilities are highlighted.

Keywords: *camouflage, engineering means, engineering and technical means, critical infrastructure facilities, important state facilities, security system.*

Statement of the problem. In modern conditions, the enemy widely uses a number of types of reconnaissance in order to identify important state facilities (CSF) and critical infrastructure facilities (CIF), as well as to determine ways to destroy them. Types of intelligence are closely interrelated and mutually complementary, providing a comprehensive picture for decision-making in various fields of activity.

The existing system for ensuring the security of CSF and CIF often demonstrates fragmentation, insufficient coordination of actions, lack of uniform standards for planning and responding to threats. This reduces the overall effectiveness of preventing, detecting and neutralizing threats at the early stages of their implementation. Therefore, there is a need to form and implement a holistic set of measures aimed at ensuring the sustainable functioning of the CIF and CSF, first of all, it is the use of modern engineering and ETMP, physical protection, camouflage, as well as coordination of actions between units of the Security and Defense Forces of Ukraine.

In this regard, it is of particular importance to improve the set of measures of the facility security system for the organization of physical, engineering, engineering and technical and special protection. The complex of these measures should ensure the implementation of tasks to prevent unauthorized entry, terrorist attacks, leakage of confidential information, as well as guarantee the technical reliability of the facility's equipment and professional training of personnel. However, the effectiveness of this system depends on the level of coherence and integration of all components into a single security system.

For the effective functioning of the security system of CSF and CIF, it is necessary to comprehensively use engineering and technical means of protection (ETMP) with engineering measures to strengthen the security of facilities, as well as to carry out additional measures to maintain camouflage discipline. Such means include video surveillance and access control systems, various security alarm systems, observation posts (positions), shelters for personnel, equipment of barriers and camouflage. It is important to understand that their effectiveness is achieved only if all elements of the system interact as a single complex. Ignoring individual components, in particular camouflage ones, or vice versa, reducing the level of engineering equipment under the pretext of increasing stealth leads to a weakening

of the overall security of the object. Therefore, the technical equipment and material support of security measures should be based on a systematic approach that takes into account both the requirements for physical security and the need to minimize unmasking signs in the conditions of modern hybrid warfare.

Ensuring the security of the CSF and CIF requires an integrated approach and coordinated interaction between all components of the security and defense sector of Ukraine.

Therefore, there is a need to improve approaches to the choice of location, camouflage, engineering equipment of ETMP, adapted to the realities of today, using the experience gained during the ongoing Russian-Ukrainian war. Such approaches will ensure the selection of a number of expedient components of the security system of CSF and CIF, taking into account their features.

Analysis of recent research and publications. A review of scientific publications on the organization of a set of measures for the security of important state facilities and critical infrastructure facilities, in particular in Ukraine, is carried out. The authors of the work [1] prove that the main reasons that negatively affect the reliability of civil protection of CIF are the following: incompleteness of initial data for the development of a technical solution; incomplete substantiation of the descriptions of the technical solution and in in some cases – non-compliance of regulatory documents with the conditions of construction of the CIF, in particular with the conditions of the special period. The article [2] provides scientific research on the reasons that negatively affect the reliability of the protection of the CIF under martial law and the direct impact of hostilities, as well as the shortcomings that arise during the development of documentation on engineering and technical means for the protection of the CIF. The scientific work [3] highlights the distribution of elements of the CIF of the energy industry for engineering protection by priority, proposes three types of engineering protection of these objects and considers organizational and technical aspects of building a system for ensuring the safety of objects. The author of the article [4] proposed methodological approaches to determining the priority of CIF protection and directions for further development of the CIF protection system in Ukraine. In the article [5] the level of cybersecurity of the unit of the Ministry of Defense of Ukraine was determined, on the basis of the results obtained, practical recommendations were formed to ensure cyber security to the required level, and a methodology for assessing the security of the cyberspace of the CIF was proposed.

These publications highlight a number of shortcomings in the justification of technical solutions for the construction of CIF in accordance with martial law, in the development of documentation for CIF and their priority; directions for further development of CIF are indicated and recommendations for ensuring cyber security are developed.However, in the current governing documents and considered works [1–5], there is a lack of attention to the organization and implementation of a set of measures to ensure the security of the CSF and CIF by units and subdivisions of the Security and Defense Forces of Ukraine.

The purpose of the article is analyzing modern approaches to the organization of a full range of measures to ensure the security of critical infrastructure facilities, in particular on engineering equipment, the use of engineering and technical means of protection and camouflage of critical infrastructure facilities in Ukraine, taking into account the experience of performing similar tasks by units of the Security and Defense Forces of Ukraine, as well as outlining the directions for improving the security system of the facility with the use of the latest technologies and means.

Summary of the main material. The problem of masking objects goes beyond minimizing the unmasking features of prohibited areas, so its solution is not only the prerogative of units of the Security and Defense Forces of Ukraine. This problem covers a wide range of issues, such as: protection from possible enemy threats, obtaining reliable data by the enemy about the ownership of the object, its purpose and nature of activity, minimizing the unmasking signs of its production cycle in the security system. preservation of the status of the object as such that is not a priority for foreign intelligence agencies. The tasks of camouflage of objects are solved by the competent authorities of the Security and Defense Forces of Ukraine.

The purpose of masking CSF and CIF is to mislead a potential enemy regarding the location of objects with their complete concealment or concealment of their characteristics and activities. Complete concealment of an object means depriving enemy reconnaissance of the ability to detect its location, location and purpose. At the

same time, it is necessary to take into account a number of unmasking features, as well as the possibility of using many types of enemy reconnaissance means, in particular: optical, radar, radio and radio engineering, pyrometric, infrared, acoustic, radiation, etc. It is also necessary to take into account the capabilities of the enemy's intelligence agents.

That is why a rather dubious approach to the decision to mask existing facilities by removing (eliminating) prohibited zones or at least their main elements is proposed. Given that many of these objects have already been recorded by the enemy's intelligence agencies, they rather need to strengthen the existing prohibited areas with the newest, more reliable technical means of protection. At the same time, it is necessary to improve the tactics of the Security and Defense Forces of Ukraine regarding the protection and defense of important facilities.

The conclusion that the objects that are taken under protection need to be masked in prohibited areas seems to be controversial if this problem is considered from the point of view of masking the object as a whole [6, 7]. If, according to the characteristic features of certain structures of the object to be taken under protection, the nature of its activities is almost completely revealed, then it is not advisable to reduce the reliability of its protection during the development of the project of this object by refusing to build a modern complex of ETMP in its prohibited zone.

For example, individual objects are determined by the nature of structures: test benches, pipelines, lightning rods, railway communications, embankment, power lines, large transformer substations, reservoirs, etc. Therefore, at such facilities, the presence of prohibited zones, as well as equipment with the ETMP complex, adds little to the disclosure of their purpose, nature and production. In addition to the above, there are a number of facilities, the destruction of which will harm the country's economy or there is a risk of creating a radioactive contamination zone (RCZ). One of the likely options for causing damage by the enemy is the use of special units, so it is necessary to take measures in advance to timely detect and neutralize sabotage groups, which is primarily associated with the strengthening of prohibited areas with engineering barriers and technical means of detection, including to the detriment of camouflage.

Certain elements of engineering and ETMP [8, 9] prohibited zones (control strip, security lighting, roads along which security forces and means move, engineering barriers and obstacles, lines of signal systems and means of detection, etc.), servicemen serving in the uniform of the Security and Defense Forces of Ukraine are also unmasking signs. However, it is not always advisable not only to completely abandon them in order to camouflage the protected object, but even to reduce their number and composition. The rejection of some elements of the ETMP reduces the reliability of the protection of the object, while focusing on the primitive equipment of the prohibited zones in case of preserving the unmasking features of the object and personnel will not increase the camouflage of the object [10].

Engineering and technical means of protection created by the purposeful work of specialized enterprises and state institutions responsible for the security of objects in recent years, taking into account practical experience, are an important component of the reliability of protection of objects. The applied ETMP provide [8]: the complexity of visual observation of the specifics of work, structures, etc., on the territory of objects; timely notification of the guards about overcoming the guard line and determining the direction of the violator's actions; restraining the actions of violators during overcoming prohibited zones and moving them in the direction of protected objects (restricted premises); identification of violators and determination of the intention of their actions; creating conditions for successful tactical actions of the Security and Defense Forces of Ukraine.

To reduce the unmasking factors of the ETMP in the prohibited zone as an important component of the facility security system, a number of factors must be taken into account in a strictly differentiated, non-standard manner, in particular: reliability of the facility's security [11]; purpose of the object and possible threats to its security; requirements for the protection and security of the object depending on the type of possible threats and risks [12]; the presence of unmasking features in the object; the cost of the ETMP complex and the maintenance of security in general; approaches to the problem of masking objects are proposed [13].

According to the status of the object, the article proposes the following classification of objects: 1) with restriction of admission; 2) with enhanced control; 3) with comprehensive security.

1. An object that is guarded (taken under protection) has no other unmasking features that reveal its purpose, except for those that are inherent in its security system (with restriction of admission). In this case, it is necessary to refuse to organize the protection of the object using the prohibited zone, equipping it only with the main barrier; in the restricted premises of the facility, the security service shall be supported by units in civilian clothes. The protection of the object should be carried out in the following way: security buildings, workshops, premises should be equipped with two or three lines of the ETMP, video surveillance and engineering means; to guard guards at checkpoints (checkpoints) without them carrying out patrols and other actions that may lead to unmasking of objects, and during non-working hours – by the method of operational duty; Surveillance of the territory should be carried out secretly by the forces of the units involved in the protection and defense of the object and the unit of the object's regime.

2. Against the background of other unmasking signs that reveal the nature of the object, the features characteristic of the object security system along the perimeter significantly prevails, their reduction (with increased control) is required. At the same time, it is necessary to increase the reliability of the protection of buildings, workshops and premises on the territory of the object by increasing the number of personnel of the unit guarding the object, or by involving other personnel in the protection and defense of the object. units of the Security and Defense Forces of Ukraine. At the same time, the prohibited zone should be equipped with a limited number of ETMP with means that will primarily detect the facts of penetration of the intruder, in certain directions with the installation of engineering barriers and obstacles in compliance with the camouflage regime. It is proposed to organize the security of the object as follows: security buildings, workshops and premises should be equipped with two or three lines of the security guards, video surveillance systems and other engineering means. Security at the checkpoint should be provided by guards without involving them in patrolling or other actions that can reveal the location of the object. During non-working hours, security should be carried out by operational duty. Control over the territory is provided secretly units involved in the protection and defense of the facility, as well as special regime units of the facility. As a result of the use of automated access systems for employees (transport) at the facilities, large human resources are released, which were previously involved in the passage of employees and transport during service at the checkpoint.

3. Objects where the security system does not significantly affect the disclosure of the nature and purpose of the object and where it is not advisable to reduce the unmasking features of the security system must be equipped with a certain complex of security protection systems (with complex security). Security at these facilities can be carried out by such methods or a combination of them [11] as: service by guards at the checkpoint, certain areas of the perimeter of the object and/or its security premises, response by guards to illegal encroachments against the object, as well as to violations of access or intra-facility regimes; operational duty of the guard, i.e. ensuring the detection of people or objects by the personnel of the guard along the perimeter of the object and/or in its security premises using detection and video surveillance means. Therefore, the conditional classification of objects by methods of protection, the degree of equipment of their ETMP and by the number of posts and personnel involved in the protection and defense of objects is determined by the order [11].

Since the masking of the elements of the security system is closely related to the reliability of the protection of the object and depends primarily on the regime of the object as a whole or on its individual subdivisions, the definition of the system for ensuring the security of the object should be approached from the position of the initial classification of objects proposed in the article.

Let us present the identified elements of the ETMP according to the degree of minimization of their unmasking factors.

1. Control and trace strips (CTS). They have the most pronounced unmasking character, since the surface is specially prepared and formed, therefore they need to be replaced with natural CTS. Natural CTS merges with the background of the environment, there are no unmasking signs of artificial CTS, and if lawns are arranged on the territory of the facility, then the CTS will be a natural continuation of these lawns and will ensure the detection of traces of penetration of violators, if any. It is also possible to completely abandon the CTS if the prohibited area is provided with reliable signaling means that make it possible to determine

the direction of penetration of violators and the means of their identification using photo, video equipment and artificial intelligence (AI).

2. Lighting system in the prohibited zone as the next most important element in unmasking. It needs modernization and maximum approximation to the environment in terms of external signs. It is advisable first of all to abandon floodlight lighting, as well as all options for security lighting systems combined with detection means. The illumination of the prohibited zone should not exceed the illumination of other territories, objects located nearby, so that it is impossible (difficult) to identify the perimeter of the object by their configuration. To monitor the state of the CTS and other elements of the prohibited zone, it is necessary to use night vision, video surveillance, and AI.

3. Routes of movement of guards, and in some cases – paths of squads, especially permanent ones, having artificial turf and located in the prohibited zone. They need to be minimized or abandoned altogether. The solution of the issue is the maximum use of intra-facility roads, and in some cases their special (secretive) construction, primarily in remote and vulnerable places located directly close to the prohibited zone. This issue must be resolved at the stage of developing acts of the interdepartmental commission and the draft of the ETMP.

4. Engineering structures, barriers and obstacles, which, when traditionally located in prohibited areas, are an essential unmasking element of the security system. The refusal to use wire fences, in particular as the main fence and the fence of the prohibited zone, emphasizes civil affiliation, since ordinary state facilities for the most part do not have such fences, the most common version of the main fence is made of reinforced concrete structures. At this time, there are many more modern options, such as decorative fences made of composites, electronic or sensory perimeters, etc. As an internal fence of the prohibited zone, you can use "hedges", which, if properly located and cared for, can serve as an obstacle, while being a natural continuation of green spaces in the form of ornamental shrubs on the territory of the object. In remote and vulnerable areas, it is recommended to use engineering obstacles, namely: inconspicuous wire interference, wire mesh on low stakes, wire garlands and spirals, etc. The above engineering obstacles are located on the surface of the earth and masked with the help of special means, vegetation cover with properties for local objects. To solve this problem, it is necessary to effectively use mobile complexes of technical means of protection, as well as reconnaissance location complexes.

5. Detection means and signal-barrier systems in prohibited areas of objects with enhanced control. It is extremely necessary to revise the tactics of using detection means and signal-blocking systems, excluding means with a large and poorly masked linear part of signal-blocking systems [8].

Since the main barrier for violators at the facilities is the main fence, the signal line must pass through it, and the sensitivity zone of the detection tool is located in such a way as to fix the intruder in the process of overcoming the main fence. It is also recommended to use two alarm lines. The first line is along the top of the main fence, and the second is in the ground version or underground. At the same time, in addition to reliably determining the direction of movement of the violator, it is possible to fix a digging under the main fence.

In view of the above, we will form the following proposals.

1. Masking of objects guarded by units of the National Guard of Ukraine and other military formations is an important task, and it must be carried out taking into account the specifics of the object and compliance with the requirements for ensuring the reliability of their protection. To accomplish this task, scientific approaches and practical application are required in accordance with experience and scientific progress.

2. Solving the problem of masking objects, and first of all their security systems, requires reviewing the equipment of the protected objects used during the protection of the prohibited zone of the protected object.

3. It is necessary to fundamentally revise the known approaches to engineering and technical support of security in order to achieve a qualitative improvement of the system of protection of objects, which ensures its reliability in combination with other important factors, in particular, a high level of masking of the object. The lack of a centralized structure in Ukraine responsible for the development of technical means of protection and assessment of their operational characteristics (including camouflage properties) for the needs of all interested ministries and departments, as well as an insufficiently developed industrial base that would ensure the production of modern means and

systems of protection, are one of the main obstacles to solving this problem.

There is a need to improve a specialized industry capable of ensuring the development, serial production and implementation of modern technical security equipment that will meet the level of the world's best analogues.

Investing in the development of this industry is economically feasible, since its products have a stable and almost inexhaustible sales market (in particular, automated access control systems can be used not only in CSF and CIF, but also in the civilian sector), and will also contribute to the optimization of the use of human resources by reducing the need for protection by traditional means.

4. At present, it is expedient to raise the issue of placement in prohibited and restricted zones of industrial sites (where the perimeter security system is already being implemented) not only traditional signaling means and systems, but also additional complex solutions that are actively used by foreign practices [14, 15]: radio broadcasting, photoelectronic and acoustic means of psychological influence, automatic shooting simulation installations, LiDAR-based systems, radar sensors, fiber-optic detectors and thermal imaging cameras for early detection of violators, guided unmanned aerial vehicles and autonomous robotic patrol systems (UGV/drones**)**, as well as laser means such as Dazzler for psychological or sensory deterrence.

The use of such systems is a more effective means of apprehending an offender within the prohibited zone and at the same time much more economical compared to the deployment of full-fledged engineering boundaries of mechanical detention.

The probability of hitting an offender who knowingly or accidentally found himself in the area of action of such means does not exceed the risk of being hit by firearms in service with security units.

In the process of organizing the protection and defense of facilities in peacetime and under martial law, in order to counter sabotage threats, it is advisable to consider the possibility of using modern high-tech means for a wider range of objects. These include: electronic barriers with integrated sensors, automated combat modules with remote control or autonomous target detection mode, active protection systems based on microwave or acoustic exposure, intelligent anti-penetrating systems using artificial intelligence, as well as robotic patrol platforms and reconnaissance drones capable of detecting and deterring the enemy without involving significant human resources.

Conclusions

Therefore, in the current conditions of large-scale armed aggression, growing activity of sabotage and reconnaissance groups and fire damage by enemy aircraft, the issue of comprehensive security of critical infrastructure facilities and important state facilities is of priority importance. The article substantiates the need for a systematic approach to the organization of the protection of such objects, which should be based on a combination of traditional and modern engineering and engineering means of protection, means of camouflage, video surveillance systems, radar and sensor monitoring, etc.

Masking important state and critical infrastructure facilities is a multidimensional problem that goes beyond just engineering or organizational solutions. It must take into account all the factors of unmasking – from the characteristic elements of objects to the activities of security units, while maintaining the reliability of the security system.

Abandoning prohibited areas in order to increase camouflage is a controversial approach, as it leads to a decrease in the level of security. Instead, it is advisable to modernize them by integrating the latest engineering and technical means of protection and detection systems to reduce unmasking factors.

Classification of objects (with limited access, with enhanced control and with comprehensive security) – allows for a differentiated approach to the organization of camouflage and security, optimizing the consumption of resources and the level of use of engineering and technical means of protection.

Unmasking elements of engineering and engineering and technical means of protection (control and trace strips, lighting, traffic paths, engineering barriers, detection systems) need purposeful improvement. This is possible by replacing artificial elements with natural ones (for example, "hedges"), the use of hidden sensor systems, the use of natural landscape and high-tech means (artificial intelligence, video analytics, LiDAR, fiber-optic sensors).

One of the important factors of effectiveness is the integration of deterrence and threat detection technologies, including acoustic, electronic, photoelectronic, robotic, and unmanned platforms [14]. Units of the Security and Defense Forces of Ukraine need uniform standards, methodological recommendations and technical support adapted to the conditions of martial law. No less important is the creation of a single center for the development, testing and implementation of engineering and technical means of protection, as well as the development of a national industrial base capable of meeting the needs for the latest security systems [15].

The use of modern high-tech solutions makes it possible to reduce dependence on human resources and increase the reliability of security, provided that a high level of masking of objects is maintained. As a result, for the effective protection of important state facilities and critical infrastructure facilities, it is extremely necessary not only to re-equip them, but also to revise the principles of organizing security measures, their adaptation to new challenges and security standards.

References

1. Yurchenko V. O., Sokolovskyi I. P. (2023). *Shliakhy udoskonalennia inzhenerno-tekhnichnykh zakhodiv tsyvilnoho zakhystu obiektiv krytychnoi infrastruktury v umovakh osoblyvoho periodu* [Ways to improve engineering and technical measures for civil protection of critical infrastructure facilities in a special period]. *Naukovyi visnyk. Seriia: derzhavne upravlinnia*, no. 1 (13), pp. 291–312. DOI: https://doi.org/10.33269/2618-0065-2023-1(13)-291-312 [in Ukrainian].

2. Bubela T. Z., Melnyk M. Ya., Nazarovets O. B., Rudyk Yu. I. (2024). *Analiz vyznachen ta normatyvnykh vymoh systemy zakhystu obiekta krytychnoi infrastruktury* [Analysis of definitions and regulatory requirements for critical infrastructure protection systems]. *Visnyk LDUBZhD. Seriia: tsyvilna bezpeka*, no. 29, pp. 119–127. DOI: https://doi.org/10.32447/20784643.29.2024.13 [in Ukrainian].

3. 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 for building an engineering protection system for critical infrastructure facilities in Ukraine's energy sector]. *Nauka i oborona. Seriia: aktualni pytannia natsionalnoi bezpeky ta oborony*, no. 3/4, pp. 11–16. DOI: https://doi.org/10.33099/2618-1614-2022-20-3-4-11-16 [in Ukrainian].

4. Bobro D. H. (2015). *Vyznachennia kryteriiv otsinky ta zahrozy krytychnii infrastrukturi* [Defining assessment criteria and threats to critical infrastructure]. *Stratehichni priorytety. Seriia: ekonomika*, no. 4 (37), pp. 83–93. Retrieved from: https://surl.li/szltgv (accessed 29 July 2025) [in Ukrainian].

5. Murasov R. K., Melnyk Ya. V. (2023). *Otsiniuvannia zakhyshchenosti kiberprostoru obiektiv krytychnoi infrastruktury Ukrainy* [Assessment of the cybersecurity of Ukraine's critical infrastructure facilities]. *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].

6. Puhach V. V., Chepurnyi V. P., Kurtov A. I. (2022). *Maskuvannia viisk ta obiektiv. Zakhyst vid vysokotochnoi zbroi* [Camouflaging troops and objects. Protection against high-precision weapons]. Kharkiv : VIuI NIuU imeni Yaroslava Mudroho [in Ukrainian].

7. Starukh O. S., Ovcharenko V. V., Pashchenko V. V. (2017). *Viiskovo-inzhenerna pidhotovka* [Military engineering training]. Kharkiv : NA NGU [in Ukrainian].

8. Vlasov K. V., Kazimirov O. O., Hlushchenko N. O. (2024). *Kompleksnyi inzhenerno-tekhnichnyi zakhyst obiektiv* [Comprehensive engineering and technical protection of facilities]. Kharkiv : NA NGU [in Ukrainian].

9. *Nakaz Ministerstva vnutrishnikh sprav Ukrainy "Pro zatverdzhennia Instruktsii z orhanizatsii ekspluatatsii inzhenerno-tekhnichnykh zasobiv okhorony na vazhlyvykh derzhavnykh obiektakh, yaki okhoroniaiutsia Natsionalnoiu hvardiieiu Ukrainy" № 56* [Order of the Ministry of Internal Affairs of Ukraine "On approval of the Instructions on the organization of the operation of engineering and technical security facilities at important state facilities guarded by the National Guard of Ukraine" activity no. 56]. (2017, January 26). Retrieved from: https://zakon.rada.gov.ua/laws/show/z0308-17#Text (accessed 1 August 2025) [in Ukrainian].

10. Nazarenko O. L., Holovan O. L., Rudynskyi V. V. (2025). *Shchodo pytannia otsiniuvannia vrazlyvosti obiektiv krytychnoi infrastruktury v umovakh voiennoho stanu* [On the issue of assessing the vulnerability of critical infrastructure facilities under martial law]. *Bezpeka derzhavy*, no. 1 (5), pp. 73–82. DOI: https://doi.org/10.33405/2786-8613/2025/1/5/336731 [in Ukrainian].

11. *Nakaz Ministerstva vnutrishnikh sprav Ukrainy "Pro zatverdzhennia Polozhennia pro orhanizatsiiu ta poriadok nesennia sluzhby z okhorony yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia derzhavnoi vlasnosti, vazhlyvykh derzhavnykh obiektiv, obiektiv krytychnoi infrastruktury ta spetsialnykh vantazhiv Natsionalnoiu hvardiieiu Ukrainy" № 497* [Order of the Ministry of Internal Affairs of Ukraine "On approval of the regulations on the organization and procedure for performing duties related to the protection of nuclear facilities, nuclear materials, radioactive waste, other sources of ionizing radiation owned by the state, important state facilities, critical infrastructure facilities, and special cargo by the National Guard of Ukraine" activity no. 497]. (2023, June 15). Retrieved from: https://zakon.rada.gov.ua/laws/show/z1085-23#Text (accessed 1 August 2025) [in Ukrainian].

12. Nazarenko O. L. (2025). *Osoblyvosti okhorony obiektiv krytychnoi infrastruktury pidrozdilamy Natsionalnoi hvardii Ukrainy* [Features of critical infrastructure protection by units of the National Guard of Ukraine]. Proceedings of the 2nd International scientific and practical conference *"Aktualni problemy diialnosti skladovykh sektoru bezpeky i oborony Ukrainy v umovakh osoblyvykh pravovykh rezhymiv: potochnyi stan ta shliakhy vyrishennia"* (Ukraine, Kharkiv, March 20, 2025). Kharkiv : NA NGU, pp. 370–371. Retrieved from: https://surl.li/atmtkg (accessed 1 August 2025) [in Ukrainian].

13. Zaporozhets T. V. (2024). *Derzhavna polityka u sferi zakhystu krytychnoi infrastruktury* [State policy in the field of critical infrastructure protection]. Kyiv : DKS-Tsentr [in Ukrainian].

14. Nazarenko O. L., Hodlevskyi S. O., Danko V. V., Fedorenko V. O. (2025). Protecting Ukraine's critical infrastructure from drone threats: the role of security and defence forces. *European Scientific e-Journal. Actual Issues of Modern Science*, issue 37, pp. 70–80. DOI: https://doi.org/10.47451/mil2025-04-01 [in English].

15. Nazarenko O. L., Onopriienko O. S. (2024). *Rol informatsiinykh tekhnolohii ta shtuchnoho intelektu v zakhysti obiektiv krytychnoi infrastruktury* [The role of information technology and artificial intelligence in protecting critical infrastructure]. Proceedings of the 2nd International scientific and practical conference *"Problemni pytannia taktyky dii ta vsebichnoho zabezpechennia viiskovykh formuvan i pravookhoronnykh orhaniv derzhavy v umovakh voiennoho stanu"* (Ukraina, Kharkiv, June 26, 2025). Kharkiv : NA NGU, pp. 38–39. Retrieved from: https://surl.lu/xvqmha (accessed 1 August 2025) [in Ukrainian].

The article was submitted to the editorial office on 12 August 2025

УДК 351.865

О. Л. Назаренко, С. О. Годлевський, І. В. Скакалін

ОРГАНІЗАЦІЯ КОМПЛЕКСУ ЗАХОДІВ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІДРОЗДІЛАМИ СИЛ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Проаналізовано основні підходи до маскування й оснащення інженерними та інженерно-технічними засобами важливих державних об'єктів і об'єктів критичної інфраструктури в умовах воєнного стану з огляду на досвід їх використання підрозділами Сил безпеки і оборони України для гарантування державної безпеки. Акцент зроблено на принципах поєднання природних і штучних засобів маскування з інженерно-технічними елементами охорони, а також на організації захисту з урахуванням розвідувальної діяльності противника, спрямованої на виявлення розташування важливих державних об'єктів та об'єктів критичної інфраструктури. Окремо розглянуто питання координації

та взаємодії між різними структурами Сил безпеки та оборони України під час забезпечення захисту зазначених об'єктів.

Підкреслено, що фрагментарність наявної системи безпеки важливих державних об'єктів і об'єктів критичної інфраструктури зумовлює необхідність формування цілісного комплексу заходів, який забезпечить їх сталу роботу шляхом поєднання фізичного захисту, інформаційної безпеки та скоординованої взаємодії підрозділів Сил безпеки і оборони України.

Обґрунтовано необхідність комплексного підходу до забезпечення безпеки об'єктів критичної інфраструктури через удосконалення вибору локацій, маскування, обладнання інженерними та інженерно-технічними засобами охорони, адаптованих до сучасних умов і заснованих на досвіді російсько-української війни, що дає змогу формувати оптимальні складники системи захисту важливих державних об'єктів та об'єктів критичної інфраструктури з огляду на їх специфіку.

Запропоновано класифікацію об'єктів критичної інфраструктури за рівнем охорони (з обмеженням допуску, з посиленим контролем та з комплексною охороною), що враховує особливості використання інженерно-технічних засобів охорони, рівень маскування та організацію взаємодії підрозділів безпеки.

Визначено і наведено елементи інженерно-технічних засобів охорони за ступенем зменшення їх демаскувальних чинників на важливих державних об'єктах та об'єктах критичної інфраструктури. Подано пропозиції щодо вирішення проблем маскування об'єктів і досягнення якісного вдосконалення системи забезпечення безпеки об'єкту. Обґрунтовано доцільність упровадження для ширшого кола об'єктів сучасних високотехнологічних засобів охорони та оборони, зокрема: електронних бар'єрів із сенсорами, автоматизованих бойових модулів, систем активного захисту, інтелектуальних протипроникних технологій, роботизованих патрульних платформ і дронів-розвідників, що здатні підвищити ефективність протидії диверсійним загрозам без значного залучення людських ресурсів.

Висновлено, що ефективна охорона важливих державних об'єктів та об'єктів критичної інфраструктури потребує поєднання традиційних і сучасних високотехнологічних засобів охорони та оборони, інженерних та інженерно-технічних засобів, маскування, систем відеоспостереження, радіолокаційного та сенсорного моніторингу. Замість відмови від заборонених зон їх слід модернізувати, використовуючи приховані сенсорні системи та новітні технології, адаптовані до умов воєнного стану, що дасть змогу зменшити демаскувальні чинники та підвищити надійність захисту.

Ключові слова: *маскування, інженерні засоби, інженерно-технічні засоби, об'єкти критичної інфраструктури, система забезпечення безпеки.*

Nazarenko Oleh – Candidate of Military Sciences, Associate Professor of the Department of State Security of the Educational and Scientific Institute of State Security, National Academy of the National Guard of Ukraine

https://orcid.org/0000-0001-7579-0658

Hodlevskyi Serhii – Candidate of Military Sciences, Head of the Department of Operational Training of the Educational and Scientific Institute of Vocational Education, National Academy of the National Guard of Ukraine

https://orcid.org/0000-0002-0437-7847

Skakalin Ihor – Lecturer of the Department of Tactics, Educational and Scientific Institute of State Security Support, National Academy of the National Guard of Ukraine

https://orcid.org/0009-0004-7568-5398