DOI: https://doi.org/10.26642/sas-2024-6(6)-83-89 │УПРАВЛІННЯ НАЦІОНАЛЬНОЮ
УДК 351.863(477+100):338.49-021.412.1 БЕЗПЕКОЮ

Batiuk Oleg
PhD in Law, Professor,
Lesya Ukrainka Volyn National University
https://orcid.org/0000-0002-2291-4247

Danylivskyi Leonid
Senior Lecturer of the Department of Intelligence
Kyiv Institute of the National Guard of Ukraine
https://orcid.org/0000-0003-1995-7980

Ensuring the security of critical infrastructure facilities as a component of national security: National and international experience

Abstract. In the provisions of the scientific article, the authors using general scientific methods conduct a study of scientific views, normative and legal regulation of national and international fundamental principles of ensuring the security of critical infrastructure facilities as a component of national security. The authors substantiate the proposals for amendments to the current legislation of Ukraine and subordinate regulations in terms of development and implementation of the following elements at a CI facility: document security in the form of the Provision on Handling Restricted Information; personnel security in the form of the Instruction on Personnel Security when Accessing Restricted Information and Physical Impact on the Personnel of a Critical Infrastructure Facility; physical security in the form of the Guidelines for Developing a Restricted Area Protection Plan or the Instruction for Establishing Restricted Areas at a Critical Infrastructure Facility; security of information and communication systems in the form of the Instruction for Accreditation of Information and Communication Systems for Processing Restricted Information. The authors note that in order to ensure proper quality for the implementation of comprehensive security measures, the CI operator has the right to choose the security measures to be implemented, for example, on the basis of internationally recognised security standards and industry or general national legislation. In the field of CI information security as a component of national security, we believe that it is good practice for the CI operator to select security controls to be implemented at the CI facility and to be guided by them in their daily activities based on ISO 27002: define corporate security policy; organisation of information security; asset management; personnel security; communications and operations management; access control; acquisition, development and maintenance of information systems; security incident management; business continuity management; compliance with applicable laws; review and audit of the existing integrated security management system.

Keywords: security; state; experience; protection; nation; critical infrastructure; facilities; resilience.

The relevance of the topic is determined by the fact that critical infrastructure is the backbone of the development of modern societies, and its deficient or inadequate protection can pose a threat to national security, economic, and stability states. Since the state represents the central point in any critical infrastructure protection system, its biggest interest is that critical infrastructure, irrespective of the ownership structure of a critical infrastructure facility or network, operates uninterruptedly, thus ensuring the smooth functioning of the community. From this perspective, it is necessary to raise awareness and proper understanding of the importance of critical infrastructure within the strategic management of the state and its institutions. In fact, it is impossible to develop a functional critical infrastructure protection system if stakeholders are unaware of its criticality for vital societal functions.

It should be noted that the emerging challenges of the twenty-first century security environment are influencing the way nations need to build their concept of critical infrastructure protection. Indeed, the protection of national critical infrastructures has shifted to a risk analysis-based approach focused on developing security and resilience, hence the focus on critical infrastructure security and resilience (CISR) [19].

The methodological basis of this article is the use of general scientific and special scientific methods of cognition. In particular, the author uses dialectical methods of cognition (abstraction, identification of the relationship between the general, the particular, and the individual, and also between the part and the whole), the method of system analysis, and formal logical and formal legal methods. The methods of classification and systematization were used to summarise the legislative, regulatory documentation, and scientific literature on the topic of the article. The application of the historical and legal method allowed analysis of the genesis of approaches to defining the concept of CI object security as a component of national security in the scientific

literature, regulatory legal acts, and international scientific research. Defining and characterizing the levels of CI object security in European countries, as well as the subjects of CI object security protection in Ukraine, were carried out using the formal logical method and the method of system-structural analysis.

Scientific research on certain aspects of critical infrastructure security is disclosed in the works of such national scientists as D.S. Biriukov, D.G. Bobro, S.G. Bratel [3], I.V. Gora, M.B. Domaratsky, O.P. Yermenchuk [4], G.Y. Zubko, V.V. Krykun [5], S.I. Melnyk [2], P.Y. Prygunov [2], V.I. Franchuk [2] and others. It should be noted that there are still a number of unresolved problems in the field of scientific research of certain aspects of security that require further scientific research.

The purpose of the article is to study the provisions of scientific works of national and international scholars and the provisions of legal documents defining the basis for critical infrastructure security as a component of national security, with a view to determining the author's position and submitting proposals for improving the current legislation of Ukraine in terms of ensuring the security of critical infrastructure facilities as a component of national security.

Presentation of the research material and its main results. Considering the issue of critical infrastructure security as a component of national security, we consider it appropriate to note that the Law of Ukraine «On Critical Infrastructure» defines the concept of critical infrastructure security as a state of critical infrastructure security, which ensures the functionality, continuity of operation, recoverability, integrity and resilience of critical infrastructure [1]. It should also be noted that Article 1 «Definition of Basic Terms» of the Law of Ukraine «On Critical Infrastructure» clearly regulates the definition of critical infrastructure objects – infrastructure objects, systems, their parts, and their aggregate, which are important for the economy, national security and defence, the disruption of which may harm vital national interests [1]. However, it should be noted that the current legislation of Ukraine does not define a clear understanding of the concept of CI security, by which we mean all activities of state and civil institutions aimed at the timely detection, prevention and neutralization of threats to critical infrastructure, as well as minimization and elimination of consequences in case of their occurrence and disruption of the intended functioning.

Summarising the regulatory framework of Ukraine, which defines the provisions for ensuring the security of CI objects, it is advisable to refer to the following regulations: Decree of the President of Ukraine No. 392/2020 of 14 September 2020, which approved «National Security Strategy of Ukraine» [7], the Concept of Creation of the State System of Critical Infrastructure Protection approved by order of the Cabinet of Ministers of Ukraine No. 1009-r of 06.12.2017 [8], the Civil Protection Code of Ukraine [9], the Laws of Ukraine «On National Security of Ukraine» [10], «On the Basic Principles of Ensuring Cybersecurity of Ukraine» [11], «On Critical Infrastructure» [1], «On Physical Protection of Nuclear Facilities, Nuclear Materials, Radioactive Waste and Other Sources of Ionising Radiation» [12], «On the Legal Regime of the State of Emergency» [13], «On the Legal Regime of Martial Law» [14], «On the Functioning of the Unified Transport System of Ukraine in a Special Period» [15] and «On the Defence of Ukraine» [16]. Resolutions of the Cabinet of Ministers of Ukraine «Some Issues of Critical Infrastructure Objects» of 09.10.2020 No. 1109 [17], as amended by the Resolution of the Cabinet of Ministers of Ukraine of 16 December 2022 No. 1384 «Procedure for Classifying Objects as Critical Infrastructure» [18].

The analysis of the above-mentioned legal acts allows us to highlight such important aspects as:

- clear regulation of provisions (terms) related to critical infrastructure, such as CI security, vital functions and/or services of CI, CI protection, identification of a CI object, CI security incident, categorization of CI objects, criticality category (criteria) of a CI object, crisis situation, critical technological information, national CI protection system, unauthorized interference, CI objects, CI operator, protection of CI objects, security passport, project threat to a CI object, register of CI objects, CI operation mode, CI object criticality level, CI sector, sectoral body in the field of CI protection, CI resilience, functional body in the field of CI protection;
- disclosure of the content of the basic principles: state policy in the field of CI protection, which includes the purpose and objectives of the state policy in the field of CI protection, basic principles of functioning of the national CI protection system, levels of management of the national CI protection system;
- disclosure of the essence of critical infrastructure, which includes: classification of objects as CI, CI sectors, categorization of CI objects, register of CI objects and certification of CI objects;
- disclosure of the content of the basic principles of the national CI protection system, which include forming and implementing the state policy in the field of CI protection, subjects of the national CI protection system, modes of functioning of the national CI protection system, authorized body in the field of CI protection, functional bodies in the field of CI protection, peculiarities of individual bodies activity, which are responsible for forming and/or implementing the state policy in the field of CI protection, sectoral bodies in the field of CI protection, powers of local executive authorities (military-civilian administrations, if established) in the field of CI protection, objectives, rights and obligations of CI operators;
- disclosure of the content of the organizational principles of the national CI protection system, which include provisions on planning measures to ensure the sustainability and protection of CI objects, monitoring the level of security of CI objects, interaction of the national CI protection system with other protection systems in

the field of national security, public-private partnership in the field of CI protection, independent audit of the national CI protection system, parliamentary control in the field of CI protection, public oversight in the field of CI protection, liability for violation of legislation in the field of CI protection, financing of CI protection measures, international cooperation in the field of CI protection, risk insurance.

While analyzing the international experience of ensuring the security of critical infrastructure facilities as a component of the national security of foreign countries, we believe that it is advisable to highlight the position of Professor S.G. Bartel, who notes that the UK is one of the European leaders in the field of critical infrastructure protection. In the legislation of this country, the term «critical infrastructure» is defined as «critical infrastructure elements, namely assets, facilities, systems, networks or processes and key personnel who manage them, the loss or compromise of which could lead to significant adverse effects on the availability, integrity or provision of essential services, including those services whose destabilization could lead to significant human casualties, taking into account significant economic or social consequences; and/or significant impact on national security, national defence or the functioning of the state».

The key difference between the above wording is that it singles out a separate category of professionals who ensure the operation of critical sectors of the state and that human security is in the first place in the list of consequences. It is also important to note that in foreign practice, the definition of critical infrastructure shifts from the physical dimension of objects to their functions and services that meet the needs of society, the state, and its economy. It is worth noting that in 1999, the UK established the National Infrastructure Security Coordination Centre, which was part of the Home Office. However, in 2016, the National Cyber Security Centre was spun off from it [4, p. 24].

In his scientific work, Professor V.V. Krykun notes that in the UK, the protection of critical infrastructure is aimed at preventing terrorism and preventing the violation of cyberspace. In the UK legislation, the essence of critical infrastructure is revealed by identifying the most important elements of infrastructure. These include assets, facilities, systems, networks, processes, and key officials, the loss of which could have a detrimental impact on the availability, integrity, or provision of essential services, the disruption of which could lead to loss of life or accidents, taking into account the significant economic and social consequences for national security, national defense or the functioning of the state [5, p. 367].

In the United Kingdom, considerable attention is paid to the issue of defining critical infrastructure sectors and establishing the types of hazards to which they may be exposed. Thus, the structure of the system of ensuring the security of critical infrastructure facilities in the country covers thirteen sectors [3, p. 35].

While considering the international experience of ensuring the security of critical infrastructure, it is worth noting that in Germany, the understanding of critical infrastructure is laid down in the National Strategy for the Protection of Critical Infrastructure, according to which critical infrastructure includes organizational and physical structures and facilities that are vital for the social and economic existence of the nation to the extent that their failure or deterioration may lead to prolonged shortages of supplies, the formation of significant gaps in the state security system or other disruptions [5, p. 51].

In the Federal Republic of Germany, the Federal Ministry of the Interior is the main coordinator of critical infrastructure protection. Germany has also created an institution called Critical Infrastructure Protection (Schutz Kritischer Infrastrukturen in Deutschland), which studies infrastructure vulnerabilities and proposes strategies for its protection and policies for cooperation and collaboration between public administration and private entities.

It is worth noting that critical infrastructures may, with reference to their technical, structural, and functional specifics, be classified as vital (absolutely essential) technical basic infrastructure, on the one hand and vital (absolutely essential) socio-economic services infrastructure, on the other hand. In Germany, these include (figure 1):

Technical basic infrastructure	Socio-economic services infrastructure
Power supply	Public health; food
Information and communications technology	Emergency and rescue services; disaster control and management
Transport(ation)	Parliament; government; public administration; law enforcement agencies
(Drinking-) water supply and sewage disposal	Finance; insurance business
	Media; and cultural objects (cultural heritage items)

Figure 1

Significant interdependencies exist between these two infrastructure sectors since nearly all of the socio-economic services infrastructures largely rely on the unrestricted availability of the technical basic infrastructure. However, technical basic infrastructures, in turn, depend on socio-economic services infrastructure, such as a stable legal service or functioning first response, emergency medical, and rescue services in the event of a crisis.

A look at the ownership structure shows that, as a rule, the various infrastructures are not state-owned facilities but that the majority of them are operated and controlled by private enterprises – part of which was privatized only recently.

Increasingly, the same also goes for the many and various public infrastructure services provided at the local government level, which more and more frequently are delivered by private-sector enterprises.

As a result of this tendency towards private ownership, the responsibility for the security, reliability and availability of such infrastructure is increasingly passed on to the private sector or, at least, becomes a shared responsibility. Thus, the functions incumbent on the state and/or public authorities are primarily directed at making provisions for, or – at the most – safeguarding and controlling, the supply of goods and services in times of crisis when regular market mechanisms no longer function.

Therefore, as a precaution against, and in view of coping with, serious disruptions and severe disasters/emergencies, the requirement is for institutionalized, organized cooperation of the state and business and industry within the framework of established security partnerships.

The Federation, the Länder, and local governments are required jointly to enhance and implement critical infrastructure protection in their respective areas of responsibility. This purpose is served by a structured implementation procedure at these three tiers of government; this procedure comprises the following work packages, which in part are implemented in parallel, and is based on the cooperative approach adopted by the Federal Administration with the involvement of the other major players, i. e. operators and the relevant associations:

1. Definition of general protection targets;
2. Analysis of threats, vulnerabilities, and management capabilities;
3. Assessment of the threats involved;
4. Specification of protection targets, taking account of existing protective measures; analysis of existing regulations and, where applicable, identification of additional measures contributing to goal attainment; if and where required legislation.

These work packages are implemented primarily by the public sector, with the collaboration of the companies and operators concerned. Responsibility for coordination at the federal level lies with the Federal Ministry of the Interior;

5. Implementation of goal attainment measures primarily by means of:
• association-specific solutions and internal regulations;
• self-commitment agreements by business and industry;
• development of protection concepts by companies;
6. Continuous, intensive risk communication process (dialogue on analysis findings, assessments, protection targets and action options).

Responsibility for the implementation of work packages 5 and 6 primarily lies with the relevant companies, operators and associations, with the participation of public agencies.

For the implementation of the National Critical Infrastructure Protection Strategy, an extensive set of instruments is available in the form of programs and plans (e. g., the National Plan for Information Infrastructure Protection (NPSI) and the related implementation plans as a strategic concept for IT infrastructure protection); programs and plans (e. g., the National Plan for Information Infrastructure Protection (NPSI) and the related implementation plans as a strategic concept for IT infrastructure protection).

In conclusion we note that in order to protect the security of critical infrastructure facilities, we consider it expedient to adopt international experience and determine that each critical infrastructure facility, regardless of industry, field of activity, and form of ownership, should develop and implement the following key security elements:

- security of documents in the form of the regulation on handling restricted information;
- personnel security in the form of the Instruction on personnel security during the access to restricted information and physical impact on the personnel of the critical infrastructure facility;
- physical security in the form of Guidelines for developing a restricted area protection plan or Instruction on establishing restricted areas at a critical infrastructure facility;
- security of information and communication systems in the form of the Guidelines for Accreditation of Information and Communication Systems for Processing Restricted Information.

We believe that for the purpose of proper quality for the implementation of comprehensive security measures, the CI operator may choose security measures to be implemented, for example, on the basis of internationally recognized security standards and sectoral or general legislation, namely:

- development and implementation of measures to prevent the occurrence of crisis situations;

- development and implementation of facility-specific action plans for CI protection and resilience;
- development and implementation of civil protection engineering and technical measures during the construction and operation of CI facilities to ensure their sustainable operation in different modes;
- development, implementation and review of facility programs to counter threats at CI facilities, information security and cybersecurity programs;
- ensuring confidentiality of information in the course of processing data on CI objects in accordance with the requirements established by law;
- ensuring the restoration of CI facilities functioning in the event of accidents / failures, illegal actions, or the impact of natural phenomena.

It is advisable to pay special attention to the information security of the CI object; we believe that it is good practice for the CI operator to select security controls to be implemented at the CI object and to be guided by them in their daily activities, based on ISO 27002:

- define a corporate security policy;
- organization of information security;
- asset management;
- personnel security;
- communications and operations management;
- access control;
- acquisition, development and maintenance of information systems;
- security incident management;
- business continuity management;
- compliance with current legislation;
- review and audit of the existing integrated security management system.

References:

1. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX, редакція від 22.08.2024 [Електронний ресурс]. – Режим доступу : https://ips.ligazakon.net/document/T211882?an=1.
2. *Франчук В.І.* Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи / *В.І. Франчук, П.Я. Пригунов, С.І. Мельник* // Соціально-правові студії. – 2021. – № 3 (13). – С. 142–148. DOI: 10.32518/2617-4162-2021-3-142-148.
3. *Братель С.Г.* Забезпечення безпеки об'єктів критичної інфраструктури у Великобританії та Німеччині / *С.Г. Братель* // Матеріали VIII Міжнародної науково-практичної конференції, 15 березня. – Дніпро : ДДУВС, 2024. – Частина І. С. 35–36. DOI: 10.31733/15-03-2024/1/35-36.
4. *Єрменчук О.П.* Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія / *О.П. Єрменчук*. – Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. – 180 с.
5. *Крикун В.В.* Адміністративно-правовий механізм захисту об'єктів критичної інфраструктури в Україні : дис. … доктора юрид. наук : 12.00.07 / *В.В. Крикун*. – Харків, 2021. – 453 с.
6. National Strategy for Critical Infrastructure Protection (CIP Strategy) / Federal Ministry of the Interior [Electronic resource]. – Access mode : http://surl.li/odagcv.
7. Стратегія національної безпеки України : Указ Президента України № 392/2020 від 14.09.2020 р. [Електронний ресурс]. – Режим доступу : https://www.president.gov.ua/documents/3922020-35037.
8. Концепція створення державної системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України № 1009-р. від 6.12.2017 р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text.
9. Кодекс цивільного захисту України : документ 5403-VI ; редакція від 01.01.2025, підстава – 4170-IX [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/5403-17#Text.
10. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII ; редакція від 09.08.2024, підстава – 3858-IX [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text.
11. Про основні засади забезпечення кібербезпеки України : Закон України від 5.10.2017 р. № 2163-VIII ; редакція від 28.06.2024, підстава – 3783-IX [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text.
12. Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання : Закон України від 19.10.2000 р. № 2064-III ; редакція від 16.10.2022, підстава – 124-IX [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2064-14#Text.
13. Про правовий режим надзвичайного стану : Закон України від 16.03.2000 р. № 1550-III ; редакція від 18.05.2024, підстава – 3633-IX [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1550-14#Text.
14. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII ; редакція від 30.10.2024, підстава – 4042-IX [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/389-19#Text.
15. Про функціонування єдиної транспортної системи України в особливий період : Закон України від 20.10.1998 р. № 194-XIV ; редакція від 23.04.2021, підстава – 1357-IX [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/194-14#Text.

16. Про оборону України : Закон України від 6.12.1991 р. № 1932-XII ; редакція від 20.11.2024, підстава – 4068-IX [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1932-12#Text.
17. Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109 ; редакція від 24.09.2024, підстава – 1066-2024-п [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.
18. Порядок віднесення об'єктів до критичної інфраструктури : Постанова Кабінету Міністрів України від 16.12.2022 р. № 1384 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1384-2022-%D0%BF#n16.
19. Contributing to NATO's Collective Defence : Security and Resilience of Critical Infrastructure Manual Manual 1 [Electronic resource]. – Access mode : http://surl.li/buhado.

References:

1. Verkhovna Rada Ukrainy (2021), *Pro krytychnu infrastrukturu*, Zakon Ukrainy vid 16.11.2021 r. No. 1882-IX, redaktsiia vid 22.08.2024, [Online], available at: https://ips.ligazakon.net/document/T211882?an=1
2. Franchuk, V.I., Pryhunov, P.Ia. and Melnyk, S.I. (2021), «Bezpeka obiektiv krytychnoi infrastruktury v Ukraini: orhanizatsiino-normatyvni problemy ta pidkhody», *Sotsialno-pravovi studii*, No. 3 (13), pp. 142–148, doi: 10.32518/2617-4162-2021-3-142-148.
3. Bratel, S.H. (2024), «Zabezpechennia bezpeky obiektiv krytychnoi infrastruktury u Velykobrytanii ta Nimechchyni», *Materialy VIII Mizhnarodnoi naukovo-praktychnoi konferentsii*, 15 bereznia, DDUVS, Dnipro, Vol. 1, pp. 35–36, doi: 10.31733/15-03-2024/1/35-36.
4. Yermenchuk, O.P. (2018), *Osnovni pidkhody do orhanizatsii zakhystu krytychnoi infrastruktury v krainakh Yevropy: dosvid dlia Ukrainy*, monohrafiia, Dniprop. derzh. un-t vnutr. sprav, Dnipro, 180 p.
5. Krykun, V.V. (2021), *Administratyvno–pravovyi mekhanizm zakhystu obiektiv krytychnoi infrastruktury v Ukrainy*, D.Sc. Thesis of dissertation, Kharkiv, 453 p.
6. Federal Ministry of the Interior, *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, [Online], available at: http://surl.li/odagcv
7. Verkhovna Rada Ukrainy (2020), *Stratehiia natsionalnoi bezpeky Ukrainy*, Zakon Ukrainy vid 14.09.2020 r. No. 392/2020, [Online], available at: https://www.president.gov.ua/documents/3922020-35037
8. Kabinet Ministriv Ukrainy (2017), *Kontseptsiia stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury*, Rozporiadzhennia vid 6.12.2017 r. No. 1009-r., [Online], available at: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text
9. Verkhovna Rada Ukrainy (2025), *Kodeks tsyvilnoho zakhystu Ukrainy*, dokument 5403-VI, redaktsiia vid 01.01.2025, pidstava – 4170-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/5403-17#Text
10. Verkhovna Rada Ukrainy (2018), *Pro natsionalnu bezpeku Ukrainy*, Zakon Ukrainy vid 21.06.2018 r. No 2469-VIII, redaktsiia vid 09.08.2024, pidstava – 3858-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text
11. Verkhovna Rada Ukrainy (2017), *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy*, Zakon Ukrainy vid 5.10.2017 r. No. 2163-VIII, redaktsiia vid 28.06.2024, pidstava – 3783-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text
12. Verkhovna Rada Ukrainy (2000), *Pro fizychnyi zakhyst yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia*, Zakon Ukrainy vid 19.10.2000 r. No. 2064-III, redaktsiia vid 16.10.2022, pidstava – 124-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/2064-14#Text
13. Verkhovna Rada Ukrainy (2000), *Pro pravovyi rezhym nadzvychainoho stanu*, Zakon Ukrainy vid 16.03.2000 r. No. 1550-III, redaktsiia vid 18.05.2024, pidstava – 3633-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/1550-14#Text
14. Verkhovna Rada Ukrainy (2015), *Pro pravovyi rezhym voiennoho stanu*, Zakon Ukrainy vid 12.05.2015 r. No. 389-VIII, redaktsiia vid 30.10.2024, pidstava – 4042-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/389-19#Text
15. Verkhovna Rada Ukrainy (1998), *Pro funktsionuvannia yedynoi transportnoi systemy Ukrainy v osoblyvyi period*, Zakon Ukrainy vid 20.10.1998 r. No. 194-XIV, redaktsiia vid 23.04.2021, pidstava – 1357-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/194-14#Text
16. Verkhovna Rada Ukrainy (1998), *Pro oboronu Ukrainy*, Zakon Ukrainy vid 6.12.1991 r. No. 1932-XII, redaktsiia vid 20.11.2024, pidstava – 4068-IX, [Online], available at: https://zakon.rada.gov.ua/laws/show/1932-12#Text
17. Kabinet Ministriv Ukrainy (2020), *Deiaki pytannia obiektiv krytychnoi infrastruktury*, Postanova vid 09.10.2020 r. No. 1109, redaktsiia vid 24.09.2024, pidstava – 1066-2024-p, [Online], available at: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text
18. Kabinet Ministriv Ukrainy (2022), *Poriadok vidnesennia obiektiv do krytychnoi infrastruktury*, Postanova vid 16.12.2022 r. No. 1384, [Online], available at: https://zakon.rada.gov.ua/laws/show/1384-2022-%D0%BF#n16
19. *Contributing to NATO's Collective Defence : Security and Resilience of Critical Infrastructure Manual Manual 1*, [Online], available at: http://surl.li/buhado

Батюк О., Данилівський Л.

Забезпечення безпеки об'єктів критичної інфраструктури як складова національної безпеки: вітчизняний та міжнародний досвід

Анотація. У положеннях наукової статті автори за допомогою загальнонаукових методів проводять дослідження наукових поглядів, нормативно-правового регулювання вітчизняних та міжнародних основоположних засад забезпечення безпеки об'єктів критичної інфраструктури (надалі – КІ) як складової національної безпеки. Автори обґрунтовують пропозиції щодо внесення змін до чинного законодавства України та підвідомчих нормативно-правових актів, в частині розроблення та впровадження на об'єкті КІ таких елементів, як: безпека документів у вигляді Положення щодо поводження з інформацією з обмеженим доступом; безпека персоналу у вигляді Інструкції з безпеки персоналу при доступі до інформації з обмеженим доступом та фізичним впливом на персонал об'єкта критичної інфраструктури; фізична безпека у вигляді Керівництва з розробки плану захисту зони обмеженого доступу чи Настанови щодо встановлення зон обмеженого доступу на об'єкті критичної інфраструктури; безпека інформаційно-комунікаційних систем у вигляді Настанови з акредитації інформаційно-комунікаційних систем для обробки інформації з обмеженим доступом. Автори зазначають, що з метою належної якості для впровадження комплексних заходів безпеки оператор КІ має право обрати заходи безпеки, які необхідно впровадити, наприклад, на основі міжнародно визнаних стандартів безпеки та галузевого або загальнонаціонального законодавства. У сфері інформаційної безпеки об'єкта КІ як складової національної безпеки вважаємо, що належною практикою є обов'язковий вибір оператором КІ засобів контролю безпеки, які варто впроваджувати на об'єкті КІ та керуватися ними у повсякденній діяльності, на основі ISO 27002: визначення політики корпоративної безпеки; організація інформаційної безпеки; управління активами; кадрова безпека; комунікації та управління операціями; контроль доступу; придбання, розробка та обслуговування інформаційних систем; управління інцидентами безпеки; управління безперервністю бізнесу; дотримання чинного законодавства; огляд та аудит діючої інтегрованої системи управління безпекою.

Ключові слова: безпека; держава; досвід; захист; нація; критична інфраструктура; об'єкти; стійкість.

Стаття надійшла до редакції 20.10.2024.