UDC 340:007
DOI: 10.56215/naia-chasopis/2.2023.74

Protection of critical infrastructure as a component of Ukraine's national security

Ihor Yefimenko*
PhD in Law
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-6684-7760

Andrii Sakovskyi
Doctor of Law, Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0003-0762-859X

Yevhen Bilozorov
PhD in Law, Associate Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-7824-6786

Abstract
The relevance of the subject under study is conditioned upon the scientific originality and practical significance of the problematic aspects of the protection of critical infrastructure as a component of the national security of Ukraine, specifically, regarding the creation and functioning of the national system of its protection. Given the fact that the term "critical infrastructure" is relatively new for Ukrainian legislation, a comprehensive list of objects included in its system has not yet been formed, and the optimal algorithms for ensuring their security have not been determined. The purpose of this study was a comprehensive investigation of Ukrainian legislation in the field of national security, which determines the legal and organizational foundations of the creation and functioning of the national critical infrastructure protection system, as well as obtaining scientific results in the form of conclusions aimed at optimizing the implementation of critical infrastructure protection. The methodological tools of the study included the hermeneutic method of learning social and legal phenomena, analytical, dogmatic, and generalization method. Considering the European integration processes of Ukraine, scientifically sound proposals were provided to improve the national legislation in the field of critical infrastructure protection according to international legal acts that govern issues of safety and protection of critical infrastructure objects. The term "critical infrastructure" was studied, the state of scientific developments regarding its protection was analysed, the algorithm of actions to ensure its security was analysed and determined, factoring in the Ukrainian political and military situation in the state

Keywords:
life support of the state and society; vital functions and/or services; national protection system; subjects and objects of protection; functions of the state; negative consequences; emergencies

Article's History:
Received: 30.03.2023
Revised: 01.06.2023
Accepted: 26.06.2023

Suggest Citation:
Yefimenko, I., Sakovskyi, A., & Bilozorov, Ye. (2023). Protection of critical infrastructure as a component of Ukraine's national security. *Law Journal of the National Academy of Internal Affairs*, 13(2), 74-85. doi: 10.56215/naia-chasopis/2.2023.74.

*Corresponding author

Introduction

At the national level, the issue of the protection of critical infrastructure (hereinafter referred to as the PCI) received special public resonance with the beginning of large-scale Russian military aggression. Thus, according to the statistics of the Ministry of Defence of Ukraine (97% of Russian targets…, 2022), in just nine months of the war, Russia, a state in violation of international law, launched over 16,000 missile strikes on various Ukrainian infrastructure objects, which caused losses in the amount exceeding a trillion US dollars. Based on these facts, the National Police alone opened more than 34,000 criminal proceedings, including those prescribed by Article 438 of the Criminal Code of Ukraine (Violation of laws and customs of war)[1].

At the scientific level, certain aspects of the PCI were reflected in the studies of many scientists and practitioners. For the most part, these studies relate to the concept of critical infrastructure (CI), statutory regulation of its activity, organization of its security and protection, as well as assessment of the main threats affecting the proper functioning of its objects. Analysing the concept of CI, O. Yermenchuk (2017) and M.N. David (2018) attributes to its content "a complex of extremely important objects of the national infrastructure, their systems and assets, whether physical or virtual, which ensure its sustainable functioning…", which corresponds to the normative definition specified in the Detective No. 114 adopted by the European Council of 2008[2].

Comparable in content, but a more specific definition is provided by O. Vergolyas (2018), who understands this term as "enterprises and institutions (regardless of the forms of ownership) … that are strategically important for the functioning of the economy and the security of the state and its population…". Considering CI as an object of state administration, O. Yaremechuk and Y. Stakhnitskyi (2022) emphasize that this category is characterized by its pertinence to the national infrastructure, which ensures the national security and defence of the country. Analogous opinions are held by S. Chumachenko and V. Trotsko (2017), stressing that a violation of the operating regime of one of its components of these elements leads to an emergency.

Investigating the category of criticality of infrastructure objects, V. Franchuk *et al*. (2021) rightly suggest considering the level of their influence on the production of goods and/or services vital for the functioning of the state and its population, which ensure the functioning of national security and defence of the state. Highlighting the main criteria according to which critical areas should be considered, D. Biryukov, S. Kondratov (2012) and S. Ducaru (2017) proposed to attribute to them a set of objectives, technologies, state and scientific structures, the violation of the regulations of which activities affects economic, socio-political, military, and environmental security. This approach is followed in the content of the Green Book on the issues of PCI prepared by the National Institute of Strategic Studies with the involvement of Ukrainian and foreign experts with the support of the NATO Liaison Office in Ukraine.

The purpose of this study was a detailed coverage of the features of the PCI as a component of the national security of Ukraine, considering the norms and provisions of the new legislation in this area of legal relations and modern realities, which determined the purpose of this study. Accordingly, the authors formulated the following tasks: to analyse the CI as a legal category and determine its place in the national security protection system of Ukraine; to identify and substantiate the main problems of the PCI, threats that affect the proper functioning of its facilities, as well as further areas for the development of its security mechanisms; to substantiate the conclusions and proposals regarding the improvement of the national PCI system and formulate priority areas for further research on the given topic.

Materials and Methods

The regulatory basis of this study included laws and sub-legislative regulations, the norms and provisions of which govern certain issues regarding the national policy in providing the PCI. Specifically, the laws of Ukraine "On the Fundamental Principles of Ensuring Cyber Security of Ukraine"[3], "On National Security of Ukraine"[4], "On Critical Infrastructure"[5], Decrees of the President of Ukraine "On Sustainable Development Goals of Ukraine for the period until 2030"[6], "On Improving Measures to Ensure the Protection of Critical Infrastructure Objects"[7], "On Urgent Measures to Neutralize Threats to the Energy Security of Ukraine and Strengthening the

[1]Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text 2341-III.
[2]Council Directive of No. 2008/114/EC "On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection". (2008, December). Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.
[3]Law of Ukraine No. 2163-VIII "On the Fundamental Principles of Ensuring Cyber Security of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.
[4]Law of Ukraine No. 2469-VIII "On National Security of Ukraine". (2018, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text.
[5]Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, November). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.
[6]Decree of the President of Ukraine No. 722/2019 "On Sustainable Development Goals of Ukraine for the period until 2030". (2019, September). Retrieved from https://zakon.rada.gov.ua/laws/show/722/2019?find=1&text=%D1%96%D0%BD%D1%84%D1%80%D0%B0%D1%81%20%D1%82%D1%80%D1%83%D0%BA#Text.
[7]Decree of the President of Ukraine No. n0014525-16 "On Improving Measures to Ensure the Protection of Critical Infrastructure Objects". (2016, December). Retrieved from https://zakon.rada.gov.ua/laws/show/n0014525-16#Text.

Protection of Critical Infrastructure"[1], Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for forming the list of information and telecommunication systems of critical infrastructure objects of the state"[2], "On some issues of objects of critical infrastructure"[3], etc.

The theoretical framework of this study included the scientific works of theoreticians and practitioners who investigated individual issues related to the subject under study. The study was based on the hermeneutic method of learning social and legal phenomena and concepts in their development and interdependence. This method helped investigated and analyse the regulations, analytical materials, concepts, and opinions of the authors on separate issues related to the subject under study. Using a descriptive-analytical, dogmatic method, an analysis of interpretations of legal categories, formulation of definitions, refinements of the terminology, proposals on the subject under study were formulated. The analysis method was used to analyse regulations that govern separate legal and organizational principles concerning the creation and functioning of the national policy on the PCI. Conclusions and suggestions were formulated using the generalization method.

Results and Discussion

Characteristics of the national critical infrastructure protection system

One of the problems of the national PCI system is that in Ukraine, a complete and final list of critical infrastructure objects (CIOs) has not yet been formed. The reason for this is, firstly, the factual lack of full-fledged functioning of the State Service for the Protection of Critical Infrastructure and Ensuring the National Stability System of Ukraine, and secondly, this process is endowed with permanent and corrective properties. That is, the CIOs are identified constantly and may change depending on the internal political and military situation in the state.

In a general sense, infrastructure, as a term, refers to general scientific concepts used in almost all spheres of human professional activity (Dubnytskyi *et al*., 2017; Melnyk & Leschuh, 2019). When interpreting this concept, the key phrase is considered, which is "a set or complex of industries, types of activities, institutions, systems, elements, etc.". That is, this refers not to any particular object, but to their structured association for solving certain tasks in a certain field of knowledge, skills, and abilities.

Considering this, the definition of term "infrastructure" depends on its particular type of activity where it is used as a certain category (Telenyk, 2020; Hankevich *et al*., 2021). Considering the multi-vector nature of this concept, the functional approach is factored in when determining the classification features of infrastructure. That is, the main areas and types of its activity, where its essence and social purpose are manifested.

Measures to ensure their safety and stability, i.e., the ability to quickly recover, are important during the operation of infrastructure facilities. This issue becomes especially relevant when it comes to critical areas of state activity, the violation of which can adversely affect the functioning of vital state institutions, and therefore harm the country's national interests. That is why, starting from the mid-1990s, in the field of protection of US national security, such a term as "critical infrastructure" appeared (President's Commission on..., 1997).

At the national, regulatory level, the issues of the PCI were first given attention in the provisions of the National Security Strategy of Ukraine "Ukraine in a Changing World" of 2007[4], where strategic goals and main tasks of national policy in the field of national security included national security in fuel and energy complex and ensuring information security at CIOs. However, this topic became especially relevant after the Russian annexation of the Crimean Peninsula. Thus, in 2015, the National Security and Defence Council of Ukraine (NSDCU) adopted a new edition of the National Security Strategy of Ukraine[5], where the principal areas of the national policy in the field of national security and defence protection included security at the CIOs.

The next step was the holding of a series of expert meetings at the National Institute for Strategic Studies and NATO member countries, based on the results of which the "Green Book on the issues of PCI in Ukraine" was drafted (Biryukov & Kondratov, 2012). In this document, for the first time, the term "critical infrastructure of Ukraine" was defined as "systems and resources, physical or virtual, that provide functions and services, the violation of which will lead to the gravest adverse consequences for the life of society, the socio-economic development of the country, and the national security". In turn, the "protection of critical

[1]The decision of the National Security and Defence Council of Ukraine No. n0001525-17 "On Urgent Measures to Neutralize Threats to the Energy Security of Ukraine and Strengthening the Protection of Critical Infrastructure". (2017, January). Retrieved from https://zakon.rada.gov.ua/laws/show/n0001525-17#Text.

[2]Resolution of the Cabinet of Ministers of Ukraine No. 563-2016-п "On Approval of the Procedure for Forming the List of Information and Telecommunication Systems of Critical Infrastructure Objects of the State". (2016, August). Retrieved from https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF#Text.

[3]Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-п "On Some Issues of Objects of Critical Infrastructure". (2020, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

[4]Decree of the President of Ukraine No. 105/2007 "National Security Strategy of Ukraine. Ukraine in a Changing World". (2007, January). Retrieved from https://zakon.rada.gov.ua/laws/show/105/2007?find=1&text=%D0%BA%D1%80%D0%20%B8%D1%82%D0%B8%D1%87#Text.

[5]Decree of the President of Ukraine No. 287/2015 "National Security Strategy of Ukraine. The Decision of the National Security and Defense Council of Ukraine". (2015, June). Retrieved from https://www.president.gov.ua/documents/2872015-19070.

infrastructure of Ukraine" was defined as "a set of measures implemented in regulatory, organizational, and technological instruments aimed at ensuring the safety and stability of critical infrastructure".

In 2016, the Government adopted the Resolution "On Approval of the Procedure for Forming the List of Information and Telecommunication Systems of the State's CIOs"[1], the provisions of which defined the concept of the State Infrastructure as "a set of state infrastructure objects that are key for the economy and industry, the functioning of society and security population, the disabling and destruction of which may have an impact on national security and defence, the natural environment, or lead to significant financial losses and human casualties". "Enterprises and institutions (regardless of the form of ownership) of such industries as energy, chemical industry, transport, banks and finance, information technology and telecommunications (electronic communications), food, healthcare, communal economy, which are strategically important for the functioning of the economy and the security of the state, society, and population".

On February 16, 2017, the National Security Service of Ukraine adopted the Decision "On urgent measures to neutralize threats to the energy security of Ukraine and strengthen the protection of CI"[2], in the operative part of which, the Ministry of Internal Affairs of Ukraine and the Security Service of Ukraine were entrusted with the responsibilities of taking urgent measures to ensure the security and protection of CI. In this context, on October 5, 2017, the Law of Ukraine "On the Fundamental Principles of Ensuring Cyber Security of Ukraine"[3], was adopted, the rules of which defined the fundamental principles of coordinating the activities of relevant entities to ensure the protection of critical information infrastructure objects.

With the adoption of the Law of Ukraine "On the National Security of Ukraine", ensuring the security of the CI was included in the main vectors of national policy in the field of national security and defence of the country, where the SBU was entrusted with the main powers to ensure the security of the CI. The content of this provision is also followed in the new edition of the National Security Strategy of Ukraine "Human security – country security", which was adopted in 2020[4], which also emphasizes the need to create an effective system of security and stability of the CI, based on a clear distribution of the subjects of its protection, as well as the limits of the implementation of their powers.

The adoption of Resolution of the Cabinet of Ministers of Ukraine No. 1109 dated 2020[5] was a major step towards the formation of the national PCI system. The provisions of this regulation approved the identification procedure (attribution of the infrastructure object to the CIOs) and the categorization of the CIOs according to four categories of criticality. These categories, depending on the set of criteria, determine the vulnerability of these objects to external and/or internal threats, the scale of the adverse consequences caused at the national, regional, municipal, or local (object) levels, the duration of restoration works and the number of forces and means involved in eliminating the consequences of an emergency.

The culminating moment in the creation and functioning of the national PCI system was the adoption of the Law of Ukraine "On Critical Infrastructure"[6] (hereinafter – the Law). This regulation defined the legal and organizational principles for the creation and functioning of the national system of the PCI, which lies in "a set of CIOs that are important for the economy, national security and defence, the malfunctioning of which can harm vital national interests." At the same time, the definition of the CI was given as simply as "the totality of CIOs", and under CIOs the legislators defined "systems, their parts and their totality, which are important for the economy, national security and defence, the malfunctioning of which can harm vital national interests". Considering the above, it is possible to reach an intermediate conclusion that CI consists of a collection and/or complexes of interconnected elements (objects), the functioning of which is vital for the state and its society, and therefore a violation of their mode of operation can have irreparable consequences for the national security and defence of the country. A distinctive feature of all these elements is that they are interconnected and interdependent. In other words, this means that the smooth operation of the banking system, the city's life support systems, the agricultural and industrial complex, as well as other important spheres of the life of the state and its institutions depends on the proper functioning of, e.g.,

[1]Resolution of the Cabinet of Ministers of Ukraine No. 563 "On the Approval of the Procedure for the Formation of the List of Information and Telecommunication Systems of Objects of Critical Infrastructure of the State". (2016, August). Retrieved from https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF#Text.

[2]Decree of the President of Ukraine No. n0001525-17 "On Urgent Measures to Neutralize Threats to the Energy Security of Ukraine and Strengthen the Protection of Critical Infrastructure. The decision of the National Security and Defense Council of Ukraine". (2017, January). Retrieved from https://zakon.rada.gov.ua/laws/show/n0001525-17#Text.

[3]Law of Ukraine No. 2163-VIII "About the Main Principles of Ensuring Cyber Security of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[4]Decree of the President of Ukraine No. 392/2020 "On the Decision of the National Security and Defense Council of Ukraine "On the National Security Strategy of Ukraine". (2020, September). Retrieved from https://zakon.rada.gov.ua/laws/show/392/2020#Text.

[5]Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-п "On Some Issues of Objects of Critical Infrastructure". (2020, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

[6]Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, November). Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text.

energy enterprises, the uninterrupted operation of the banking system, the city's life support systems, agrarian and industrial complex, as well as other important spheres of life activity of the state and its institutions.

According to the Law, the national system of PCI is divided into four levels, which are managed by authorized entities that form and implement the national policy on the PCI. A prominent place in the system of PCI subjects is occupied by the authorized body in the field of PCI, which, according to the Resolution of the Cabinet of Ministers of Ukraine dated November 12, 2022 No. 787[1], is the State Service for the Protection of Critical Infrastructure and Ensuring the National Stability System of Ukraine (the SPCI). According to its legal status, the SPCI is the central body of the executive power and the main body that forms and implements national policy in the field of the PCI and ensures the national system of stability of Ukraine.

To coordinate the actions of the subjects of the national system of PCI, the SPCI was entrusted with the authority to form and keep the CIO Register, which consists of an automated sectoral list of CIOs. After the registration of the CIO (attribution of the CIO to the relevant register), the sectoral bodies in the field of the PCI inform the operator of the CIO about this for the preparation of the appropriate safety passport, which contains information on the identification of this object, a list of measures necessary for its protection and safety, and as well as a circle of individuals responsible for communication with other subjects of the national PCI system.

The protection and stability of CI by the subjects of the national system of its protection is ensured pursuant to the modes of operation of the national PCI system defined by the Law. To the latter, the Law refers the following: regular mode (assessment of possible threats and information about them); standby mode (checking and transferring the protection system to the readiness to protect the CIO in the event of a threat); response mode (crisis response measures); recovery mode (measures taken to return the operation of the CIO to normal mode).

On November 4, 2022, the President of Ukraine signed the amendments to the Laws of Ukraine "On Critical Infrastructure" and "On the State Service of Special Communications and Information Protection of Ukraine"[2], approved by the Verkhovna Rada. According to these amendments, during the special period and for twelve months after its end, the State Service for Special Communications and Information Protection of Ukraine carries out the powers of the authorized body in matters of PCI. In a general sense, this document is a natural continuation of the national policy in the field of PCI, which helps better ensure the protection and stability of its objects in the conditions of martial law.

Objects of the national PCI system

The legal requirement for the object to be classified as a CI is to provide it with vital functions and/or obedience for the state and its society, the violation of which may lead to dangerous consequences for the national security and defence of the country. In fact, the Law refers to such functions and/or services:

Management and provision of the critical (administrative) services. The provision of administrative services is related to the exercise of authority by authorized subjects of state power (mostly executive), local self-government bodies, as well as other subjects authorized to carry out state registration, provide administrative services, etc.[3]. Energy supply (specifically, the supply of thermal energy). This refers to a set of enterprises (institutions, organizations) to produce (extraction, processing) material objects where concentrated energy is suitable for practical use by humans (Leschuk, 2017).

Water supply and drainage. This category includes a set of enterprises (institutions, organizations) servicing water circulation systems, including the production of drinking and technical water, its water supply and drainage.

Food security. That is, a set of enterprises (institutions, organizations) for the cultivation, processing, manufacturing, packaging, storage and distribution (supply) of products of plant, animal, mineral, synthetic (biotechnological) origin, used for the production of food products.

Healthcare. This sector consists of a set of healthcare facilities, including hospitals, military medical facilities, family medicine centres, health centres, dispensaries, boarding houses, sanitary-epidemiological services, donor institutions, medical laboratories, morgues, etc.

Pharmaceutical industry. This industry includes the production of medicines and medical products, their wholesale and retail trade, specialized storage, distribution.

Production of vaccines, sustainable functioning of biolaboratories. The production of vaccines is the result of a complex and lengthy production process, in specialized laboratories, which involves suitable control at all its stages. The stages of vaccine production include the research stage (vaccine development); preclinical studies of a candidate vaccine; clinical trials of

[1]Resolution of the Cabinet of Ministers of Ukraine No. 787 "On the Establishment of the State Service for the Protection of Critical Infrastructure and Ensuring the National Stability System of Ukraine". (2022, November). Retrieved from https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text.

[2]Law of Ukraine No. 3475-IV "On the State Service of Special Communications and Information Protection of Ukraine". (2006, January). Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15#Text.

[3]Law of Ukraine No. 5203-VI "On Administrative Services". (2012, September). Retrieved from https://zakon.rada.gov.ua/laws/show/5203-17?find=1&text=%D1%83%D1%80%D1%8F%D0%B4%D1%83% D0%B2%D0%B0#Text.

a candidate vaccine; registration and approval of normative documents in the relevant regulatory body; vaccine production; quality control during mass production and use (Sakhanyuk, 2020).

Information services. This sector is aimed at the proper functioning of enterprises (institutions, organizations) that carry out information activities in the form defined by law to meet the information needs of the population.

Electronic communications. That is, a set of enterprises (institutions, organizations) that ensure the functioning of information transmission and reception systems in the form of electromagnetic signals, including technological means of electronic communication and lines of electronic communication networks[1].

Financial services. This category includes a set of enterprises (institutions, organizations) that secure the operations with financial assets in cases prescribed by law[2].

Transport support. This sector includes a set of enterprises (institutions, organizations) that ensure the functioning of the transport system, which is covered by all means of transportation (aviation, sea routes, highways, railways, main pipelines) (Lordan-Perret *et al*., 2019; Zhu *et al*., 2021).

Defence, national security. This category includes two related sectors, which are critical for the functioning and life of any state. According to the national legislation, the country's defence consists of relevant systems aimed at protecting the state from external military aggression[3]. In turn, national security lies in protecting the state from potential threats of a non-military nature[4]. The objects of ensuring the national security and defence of the country are state sovereignty, constitutional order, territorial integrity, defence, economic and technological potential, cyber security, information security, state secrets, official information and, as a result, CIOs[5].

Law and order, administration of justice, detention. According to Article 19 of the Constitution of Ukraine, the legal order in Ukraine[6] is based on the principles, according to which no one shall be forced to do what is not prescribed by the law, and state authorities, local self-government bodies (their officials) shall be obliged to act only on the basis, within the limits, and in according to the procedures prescribed by law. The content of this norm reflects the equal level of all subjects of legal relations before the law without exception, which includes state authorities, local self-government bodies and their officials, enterprises (organizations, institutions) regardless of the forms of ownership, citizens, foreigners, stateless persons, including their association. In case of violation of this axiom, anyone shall be entitled to seek protection from the court, law enforcement agencies, state authorities, local self-government bodies and their officials (Perinić & Mikac, 2021; Tertyshnyk, 2022), which is also confirmed by the Decision of the Constitutional Court of Ukraine from January 30, 2003 No. 3-рп/2003[7].

Civil protection of the population and territories, rescue services. This sector includes a set of enterprises (institutions, organizations) that ensure the functioning of systems for the protection of the population, territories, the environment, material, and cultural values both in peacetime and in a special period, including the prevention of emergency situations, liquidation of its consequences, aid to victims, etc.[8]. Subjects of civil protection, depending on the territorial jurisdiction, functional purpose and assigned powers, include relevant central and local bodies of state executive power, local self-government bodies, economic entities and public organizations[9].

Space activities, space technologies and services. That is, a set of enterprises (institutions, organizations) that ensure the functioning of space activities, the purpose of which is the research and use of outer space using space technologies[10].

[1]Law of Ukraine No. 1089-IX "About Electronic Communications". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1089-20?find=1&text=%D1%81%D0%B8%D1%81%D1%82%D0%B5% D0%BC#w1_1.
[2]Law of Ukraine No. 2664-III "About Financial Services and State Regulation of Financial Services Markets". (2001, July). Retrieved from https://zakon.rada.gov.ua/laws/show/2664-14#Text.
[3]Law of Ukraine No. 1932-XII "About the Defense of Ukraine". (1991, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1932-12#Text.
[4]Law of Ukraine No. 2469-VIII "About the National Security of Ukraine". (2018, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text.
[5]Decree of the President of Ukraine No. 56/2022 "On the Decision of the National Security and Defense Council of Ukraine. Strategy for Ensuring State Security. "On the Strategy for Ensuring State Security". (2022, June). Retrieved from https://zakon.rada.gov.ua/laws/show/56/2022#Text.
[6]Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[7]Decision of the Constitutional Court of Ukraine No. 1-12/2003 "In the case on the constitutional submission of the Supreme Court of Ukraine regarding the conformity of the Constitution of Ukraine (constitutionality) with the provisions of the third part of Article 120, the sixth part of Article 234, the third part of Article 236 of the Criminal Procedure Code of Ukraine (the case of court consideration of individual resolutions of the investigator and prosecutor). Decision of the Constitutional Court of Ukraine on behalf of Ukraine". (2003, June). Retrieved from https://zakon.rada.gov.ua/laws/show/v003p710-03#Text.
[8]Code of Civil Protection of Ukraine. (2012, October). Retrieved from https://zakon.rada.gov.ua/laws/show/5403-17?find=1&text=%D0%B0%D0%B2%D0%B0%D1%80%D1%96% D0%B9%D0%BD%D0%BE#Text.
[9]Law of Ukraine No. 2469-VIII "About the National Security of Ukraine". (2018, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text.
[10]Ibidem, 2018.

Chemical industry. This sector includes a set of enterprises (institutions, organizations) that ensure the functioning of the industry for the manufacture of products from hydrocarbon, mineral, and other raw materials through their chemical processing.

Research activity. This sector is the basis of the development of the modern information and creative society. It includes such concepts as "state research infrastructure", "research production", "research infrastructure", "European research area", etc.[1]. CIOs related to this category are scientific institutions and institutions of higher education, their structural subdivisions, a set of means, resources, and related services, which are used by scientific and pedagogical staff to conduct scientific research, development, etc.

Therefore, critical infrastructure comprises not only a set of particular physical objects, such as roads, bridges, dams, power plants and their networks, manufacturing enterprises and institutional institutions, etc., but vital services for the functioning of the state, which are covered by a single political, legal, military, economic, cultural, humanitarian space. In this context, CI acts as a determinant of state functions, factually ensuring their practical implementation (Bilozyorov *et al*., 2017). In other words, this means that CI ensures the vital functions of the state in the field of national security and defence of the country.

The national nature of the implementation of its functions acquires particular importance in the life of the state (Bilozyorov, 2010). Thus, for instance, the inherent features of a modern democratic state are as follows: 1) creation of the necessary conditions for maximum preservation and development of the nation's best assets and political consolidation of society around the national idea; 2) promoting the development of spirituality, language, culture of traditions inherited from previous generations; 3) implementation of the national idea in the state-building process in the context of ensuring national security and defence.

In a general sense, national values include material and spiritual values that the nation inherited from its ancestors (Tkalya, 2022). In other words, these are any objects that are national, state property or the property of individual legal entities or individuals, and for which a special protection regime has been established, including monuments of architecture, art, culture, history, etc.

In an attempt to deprive Ukrainians of their national identity and self-awareness, over three thousand educational and cultural objects, including museums, theatres, monuments of culture and national heritage, were destroyed or damaged only during the investigated period of the full-scale war in Ukraine by the state-violator of international law etc. This is confirmed by the fact that in just one day of rocket attacks by the Russian occupying forces on the historical centre of Kyiv, which took place on October 10, 2022, the Taras Shevchenko Kyiv National University, the Bohdan and Varvara Khanenko National Museum of Art, the National Museum "Kyiv Art Gallery", National Philharmonic of Ukraine, Taras Shevchenko National Museum, National Science and Nature Museum of the National Academy of Sciences of Ukraine (Rocket attack on Kyiv…, 2022).

That is why it is proposed to supplement the Part 4 of Article 9 of the Law of Ukraine "On Critical Infrastructure" with the "eighteenth" paragraph, in which vital functions and/or services, the violation of which leads to negative consequences for the national security of Ukraine, should include the sphere of relations regarding the protection of the cultural and national heritage of Ukraine. This addition will further provide additional guarantees for the protection of cultural heritage sites of Ukraine, which are proof of the centuries-old existence of the Ukrainian nation, its history and culture.

Investigating the main problems of the PCI, we will try to substantiate the classification given by D. Biryukov & S. Kondratov (2012) referring to the scientific developments of the American researcher T. Lewis (2020), namely:

1) the importance of each of the CI sectors in general and in particular. It means that CIOs depend on each other according to the principle of action of the "domino effect", and therefore unauthorized interference in the work of one of the sectors can cause a chain reaction and cause a "cascade effect". That is, some destruction can be the cause of other related to them by the same system of CI elements.

2) security management takes place under conditions of interdependence of activities of government bodies, state and private structures, as well as regulatory and economic factors. The safety of the CIO is a complex category that depends on a range of factors of internal or external origin that affect the life activity of the CIO. That is, military aggression, natural disasters, economic crises, pandemics, activity of investment engagements, etc.

3) ineffective communication between the subjects of the protection system. This category refers to the proper organization of the interaction of the subjects of the national PCI system. The problem is that the system of CI elements is branched and dispersed throughout the country, with a considerable number of state and private structures, which, in turn, adversely affects the timeliness of the necessary data exchange between them. To correct this situation, in Ukraine, processes are taking place regarding the digitalization of society, which will further facilitate the effective exchange of information between competent subjects of the national system of information and communication technology.

4) interdependence of CI elements and sectors. Given that most CI systems have a network architecture,

[1]Law of Ukraine No. 848-VIII "About Scientific and Scientific and Technical Activity". (2015, November). Retrieved from https://zakon.rada.gov.ua/laws/show/848-19#Text.

it is necessary to protect, first of all, the main "nodes" of these systems, following the "80/20" rule, where 80% are resources that should be spent on 20% of the country's territory (Lewis, 2020). It is also suitable to use the "network theory" for organizational and physical structures. That is, when the main CI nodes are distant from each other, and the system of objects itself is divided into small parts (Alcaraz & Sherali, 2015; Denisiuk *et al*., 2016).

5) inefficient distribution of powers from PCI between central and local state authorities. The solution to this problem depends on the imperative expression in the national legislation of the provisions that determine the specific functions of each of the subjects, depending on the level of management of the national PCI system.

6) lack of a common methodical basis for determining the risks and properties of objects. Solving this problem requires conducting analytical and methodical measures for the clear formation of the registry of CIOs, identification of existing or potential risks and threats that affect their regular functioning, including ways to ensure their protection at each of the levels of functioning of the national system of CIOs.

7) insufficiently active involvement of CI operators (owners) in ensuring its protection. It is the operators who handle the identification of CIOs. This stage is the initial stage in the protection of the CIOs and allows for its necessary registration, categorization, and passporting to be carried out in the future. Therefore, the identification of CI is the main stage that affects the general mechanism of protection of critically important spheres of state activity and helps systematize the totality of CI elements and determine its main sectors to ensure their protection.

During the identification of CIOs, the following is considered: the extent of the damage caused (territorial distribution of the consequences of possible damage); the relationship between CI elements (the spread of the damage to other CI objects or sectors); the duration and nature of the impact of the damage caused (exactly how and for what time the damage caused will be manifested in connection with the violation of the regular mode of operation of the CIO); vulnerability of CIOs to the emergence of extraordinary situations of anthropogenic, natural, social, or military nature.

This category also includes the degree of severity, including damage caused and adverse consequences that may be caused in such areas as: economic security (the impact of damages on GDP, the size of direct and indirect economic losses, the share of products on the market, the number of employed workers is calculated, the amount of tax revenues); the safety of life and the health of the population (the number of people who may be injured, the number of the population that needs evacuation and the number of involved emergency and rescue services are calculated).

At the global level, there is a need for internal political and national security (considering the nature of the loss of military and political power, the authority of state institutions, violation of sovereignty and territorial integrity, etc.); security and defence of the country (considering the reduction of the defence capability and fighting capacity of the armed forces, security agencies, other law enforcement agencies and services, the possibility of disclosing information with limited access, etc.); environmental safety (the impact on ecology and the environment is calculated).

As for the main threats that affect the functioning of CIOs, at the research-to-practice level, this issue is reflected in the studies of many theoreticians and practitioners, who rightly include pandemics, industrial accidents, criminal activity, natural disasters, as well as other predictable and unpredictable factors against which the state must provide adequate protection (Chowdhury & Gkioulos, 2021; Lazari & Mikac, 2022). Considering this, the main threats to the functioning of the CIOs can be conditionally divided into five categories, namely:

1) anthropogenic. Considering the threats of this category, D. Biryukov & S. Kondratov (2012) address the fact that in Ukraine, due to the prominent level of wear and tear of the main CI nodes, there is a danger of emergencies occurring at dangerous enterprises. As an example, scientists cite some statistical data of the State Emergency Service, according to which there are over a thousand high-risk enterprises in Ukraine, accidents at which can cause unpredictable catastrophic consequences. These facilities include enterprises of the chemical and metallurgical industry, mining enterprises, enterprises of the grain processing industry, nuclear power plants, etc.[1].

2) natural. Among natural threats, scientists distinguish the following types: meteorological (snowfalls, ice, blizzards, showers, hailstorms, frosts, droughts); hydrological (floods, mudslides, floods, inundation); geological (dangerous exogenous geological processes – landslides, subsidence, and karst); heliophysical (fires) (Yermenchuk, 2018).

For instance, it is possible to cite the largest flood since independence, which occurred in 2020 in the west of Ukraine. As a result of this natural disaster, the water in the rivers rose by more than three meters, which led to the flooding of approximately three hundred settlements (Ukraine's climate is changing…, 2020).

3) social. Given the limits of the study, the authors propose to consider this and the next category of threats in greater detail in the next paper. Along with this, the main threats of a social nature that directly

[1]Cabinet of Ministers of Ukraine No. 1214-2020-п "On Approval of the Procedure for Selecting Projects to be Implemented under the Big Construction Programme". Retrieved from https://zakon.rada.gov.ua/laws/show/1214-2020-%D0%BF#Text.

affect the functioning of the CIOs are illegal activities aimed at disrupting the operation of the CIOs (its capture, sabotage, terrorist acts, theft or damage to property on which its normal functioning depends, cyber-attacks against its systems management, etc.) (Iksarova, 2010; Dreis, 2017).

4) military. According to preliminary calculations by the Kyiv School of Economics (The Security Service of..., 2023), in just ten months of the war, Ukrainian infrastructure suffered losses exceeding 138 billion US dollars. And this is without considering the illegal annexation of Crimea, the period of the anti-terrorist operation (operation of the joint forces), as well as environmental and other damages caused by Russian military aggression.

5) combined. Combined threats are threats that were caused by the action of the cascade effect when the destruction of one of the CIOs caused the destruction of other life support systems. An example is the accident at the Fukushima 1 nuclear power plant in the eponymous prefecture in Japan (In one week..., 2022). As a result of this event, due to interruptions in the power supply, there was a stoppage of railway transport, which essentially paralysed the logistics of a separate region (Hasegawa *et al*., 2016). In addition, as a result of the radioactive release of radioactive isotopes into the ocean waters, damage was caused to the ecology and the surrounding environment, which caused the evacuation of 200,000 people to a safe zone.

Conclusions

Despite the relative fragmentation of the term "critical infrastructure" in the Law, it can be defined as a set and/or complex of infrastructure objects that are vital for the economy, national security and defence of the country, and which, pursuant to the law, have undergone the identification procedure, categorization, registration, and passporting. In turn, the national system of the PCI consists of a set of relevant entities that handle the formation and/or implementation of national policy on the PCI. An inherent feature of this system is an individually complex approach to the definition of objects and subjects of the PCI, which means that each country, within its state borders and considering national interests, separately forms its own system of the PCI. Certain objects are attributed to CI according to a set of criteria, which include: performance and/or provision of important functions and/or services by these facilities; the vulnerability of these objects to external and internal threats, which can lead to grave adverse consequences, as a result of which significant (substantial) damage will be caused to the health of the population, the social sphere, state sovereignty, the economy, as well as natural resources of the national, regional, municipal, and object value; the scale and duration of the adverse consequences caused by unauthorized interference in the work of these facilities, affecting the activities of strategically important spheres of the state; the duration of measures to eliminate adverse consequences caused by unauthorized interference in the work of these objects, their impact on the functioning of other (adjacent) sectors of the CI, as well as the number of resources involved in their elimination.

Violation of the operation mode of the CIO includes those potential threats (virtual or physical), the root causes of which are both human (intentional or careless) and natural (meteorological, hydrological, geological, heliophysical) factors that lead to the emergence of a crisis situation at the CIO, which, firstly, poses a threat to the life and health of the staff of this object and/or the local population in the area where it is located, secondly, threatens the safety of citizens and/or their material situation, and thirdly, disrupts the functioning of one of elements of the life support system of the population or the country as a whole.

Issues related to the prevention, detection, termination, investigation, and solving of criminal offences, the objects of which are CIs, require special attention. Equally important are studies on the forms of ownership of CIOs, especially when it comes to the privatization of CIOs, which directly affects the defence capability and national security of the country.

Acknowledgements

None.

Conflict of Interest

None.

References

[1] 97% of Russian targets are civilians: Reznikov published the statistics of russian missile strikes. Ukrinform. (2022). Retrieved from https://www.ukrinform.ua/rubric-ato/3623683-reznikov-rf-zavdala-po-ukraini-vze-ponad-16-000-raketnih-udariv-97-cilej-civilni.html.

[2] Alcaraz, C., & Sherali, Z. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection,* 8, 53-66. doi: 10.1016/j.ijcip.2014.12.002.

[3] Bilozyorov, E., Vlasenko, V.P., Horova, O.B., Zavalnyi, A.M., Zayats N.V., & Kharchenko, N.P. (2017). *Theory of the state and law*. In S.D. Husarev & O.D. Tikhomirov (Eds.). Kyiv: Education of Ukraine.

[4] Bilozyorov, E. (2010). The Ukrainian national state: Reality or illusion. *Scientific Journal of the NPU Named After M.P. Drahomanova 18: Economics and Law,* 8, 135-142.

[5] Biryukov, D., & Kondratov, S. (2012). *Protection of critical infrastructure: Problems and prospects of implementation in Ukraine*. Kyiv: National Institute of Strategic Investigations.

[6] Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: A systematic literature review. *Information and Computer Security*, 29(5), 697-723. doi: 10.1108/ICS-07-2020-0121.
[7] Chumachenko, S., & Trotsko, V. (2017). Assessment of threats to critical infrastructure facilities. *Scientific Bulletin: Civil Protection and Fire Safety*, 1, 41-47.
[8] David, M.N. (2018). *Cyber risk of coordinated attacks in critical infrastructures*. Retrieved from https://experts.illinois.edu/en/publications/cyber-risk-of-coordinated-attacks-in-critical-infrastructures.
[9] Denisiuk, S., & Kotsar, O. (Eds.). (2016). *Energy efficiency of Ukraine. Best project ideas*. *Project "Professionalization and Stabilization of Energy Management in Ukraine"*. Kyiv: KPI named after Igor Sikorskyi.
[10] Dreis, Y. (2017). Analysis of basic terminology and negative consequences of cyberattacks on information and telecommunication systems of critical infrastructure of the state. *Protection of Information*, 19(3), 214-222. doi: 10.18372/2410-7840.19.11900.
[11] Dubnytskyi, V., Fedulova, O., & Vasyliuk, V. (2017). Regional infrastructure: Modernization, priorities and development prospects. *Economic Problems: Regional Economy*, 2, 167-168.
[12] Ducaru, S. (2017). The security of critical energy infrastructure in the age of multiple attack vectors: NATO's multi-faceted approach. *Europolity-Continuity and Change in European Governance,* 11(1), 5-20. doi: 10.25019/europolity.2017.11.1.01.
[13] Franchuk, V., Pryhunov, P., & Melnyk, S. (2021). Security of critical infrastructure facilities in Ukraine: Organizational and regulatory problems and approaches. *Social and Legal Studies*, 3(13), 142-148. doi: 10.32518/2617-4162-2021-3-142-148.
[14] Hankevich, K. Levchuk V.D., & Korolev, S.S. (2021). Peculiarities of the formation of the legal basis for the existence of critical infrastructure objects of Ukraine in the system of the Ministry of Defense of Ukraine. *Legal Scientific Electronic Journal,* 11, 79-82. doi: 10.32782/2524-0374/2021-11/15.
[15] Hasegawa, A., Ohira, T., Maeda, M., Yasumura, S., & Tanigawa, K. (2016). Emergency responses and health consequences after the Fukushima accident: Evacuation and Relocation. *Clinical Oncology*, 28(4), 237-244. doi: 10.1016/j.clon.2016.01.002.
[16] Iksarova, N. (2010). Transport infrastructure as a component of economic security of Ukraine. *Economic Space*, 36, 55-61.
[17] In one week, the damage caused to Ukraine's infrastructure during the war increased by at least $8.3 billion. (2022). Retrieved from https://kse.ua/ua/about-the-school/news/za-tizhden-zbitki-naneseni-v-hodi-viyni-infrastrukturi-ukrayini-zrosli-shhonaymenshe-na-8-3-mlrd/.
[18] Lazari, A., & Mikac, R. (2022). *The external dimension of the European Union's critical infrastructure protection programme.* Boca Raton: CRC Press. doi: 10.4324/9781003273769.
[19] Leschuk, G. (2017). Conceptual determinants of investment infrastructure of the region. *Scientific Bulletin of the International Humanitarian University. Series: Economics and Management*, 24(2), 20-24.
[20] Lewis, T.G. (2020). *Critical infrastructure protection in homeland security: Defending a Networked Nation.* Hoboken: John Wiley & Sons.
[21] Lordan-Perret, R., Wright, A.L., Burgherr, P., Spada, M., & Rosner, R. (2019). Attacks on energy infrastructure targeting democratic institutions. *Energy Policy,* 132, 915-927. doi: 10.1016/j.enpol.2019.06.025.
[22] Melnyk, M., & Leschuh, I. (2019). Development of the institutional infrastructure of business support in the region: Trends and prospects. *Efficient Economy*, 10. doi: 10.32702/2307-2105-2019.10.14.
[23] Perinić, J., & Mikac R. (2021). Protection of the critical infrastructure from terrorism: Case study of the Republic of Croatia. *IOS Press. Series: NATO Science for Peace and Security: Information and Communication Security,* 39, 235-250. doi: 10.3233/978-1-61499-478-7-235.
[24] President's commission on critical infrastructure protection. (1992). Retrieved from https://www.hsdl.org/?abstract&did=487492.
[25] Rocket attack on Kyiv: 45 buildings, cultural and educational institutions were damaged. (2022). Retrieved from https://www.ukrinform.ua/rubric-kyiv/3590339-raketnij-udar-po-kievu-poskodzeni-45-budinkiv-zakladi-kulturi-j-osviti.html.
[26] Sakhanyuk, O. (2020). *Types of vaccines and their development. Vaccination as the most effective method of protecting the population from infectious diseases*. Retrieved from https://www.dec.gov.ua/wp-content/uploads/Conference/2020/6/section/9/s9f3.pdf;
[27] Telenyk, S. (2020). The concept and content of the state critical infrastructure protection system. *Carpathian Legal Gazette*, 2(31), 112-120. doi: 10.32837/pyuv.v0i2(31).577.
[28] Tertyshnyk, V. (2022). *Constitution of Ukraine. Scientific and practical commentary.* Kyiv: Alerta.
[29] The Security Service of Ukraine prevented attempts to hack the state electronic system in the construction industry. (2023). Retrieved from https://ssu.gov.ua/novyny/sbu-zapobihla-sprobam-zlamu-derzhavnoi-elektronnoi-systemy-u-haluzi-budivnytstva-video.

[30] Tkalya, O. (2022). National interests and values as the basis for the existence and development of the national state. *Legal Scientific Electronic Journal,* 4, 58-61. doi: 32782/2524-0374/2022-4/12.
[31] Ukraine's climate is changing rapidly, and no one is ready for it. (2020). Retrieved from https://www.unian.ua/ecology/povin-v-karpatah-ukrajina-viyavilasya-negotovoyu-do-zmini-klimatu-11060969.html.
[32] Vergolyas, O. (2018). *Reforming the protection system and increasing the stability of Ukraine's critical infrastructure in terms of current threats*. Retrieved from https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html.
[33] Yaremechuk, O., & Stakhnitskyi, Y. (2022). Theoretical approaches to defining the definition of critical infrastructure as an object of public administration. *Public Administration and Customs Administration*, 1(32), 76-82. doi: 10.32836/2310-9653-2022-1.13.
[34] Yermenchuk, O. (2017). Normative and legal regulation of activity in the sphere of protection of national critical infrastructure: Analysis and generalization of the US rule-making practice. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*, 3, 135-140.
[35] Yermenchuk, O. (2018). *Basic approaches to the organization of critical infrastructure protection in European countries: Experience for Ukraine.* Dnipro: Dnipropetrovsk State University of Internal Affairs affairs.
[36] Zhu, H., Zhang, C., Ramirez-Marquez, J.E., Wu, S., & Monroy, R. (2021). The integration of protection, restoration, and adaptive flow redistribution in building resilient networked critical infrastructures against intentional attacks. *IEEE Systems Journal*, 15(2), 2959-2970. doi: 10.1109/JSYST.2020.3039466.

Захист критичної інфраструктури як складова національної безпеки України

Ігор Єфіменко
Кандидат юридичних наук
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-6684-7760

Андрій Саковський
Доктор юридичних наук, професор
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0003-0762-859X

Євген Білозьоров
Кандидат юридичних наук, доцент
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-7824-6786

Анотація
Актуальність теми дослідження обумовлена науковою новизною та практичною значущістю проблемних аспектів захисту критичної інфраструктури як складової національної безпеки України, зокрема щодо створення та функціонування національної системи її захисту. З огляду на те, що термін «критична інфраструктура» для українського законодавства є порівняно новим, вичерпного переліку об'єктів, які входять до її системи, ще не сформовано, а оптимальних алгоритмів забезпечення їх безпеки не визначено. Метою статті є комплексне дослідження українського законодавства у сфері національної безпеки, що визначає правові й організаційні засади створення та функціонування національної системи захисту критичної інфраструктури, а також отримання наукових результатів у вигляді висновків, спрямованих на оптимізацію реалізації захисту критичної інфраструктури. Методологічним інструментарієм дослідження є герменевтичний метод пізнання соціальних і правових явищ, аналітичний, догматичний, а також метод узагальнення. Зважаючи на євроінтеграційні процеси України, надано науково обґрунтовані пропозиції щодо вдосконалення національного законодавства у сфері захисту критичної інфраструктури відповідно до міжнародно-правових актів, які регулюють питання безпеки та захисту об'єктів критичної інфраструктури. Досліджено поняття «критична інфраструктура», здійснено аналіз стану наукових розробок щодо її захисту, проаналізовано та визначено алгоритм дій із забезпечення її безпеки з урахуванням внутрішньополітичної та воєнної ситуації в державі

Ключові слова:
життєзабезпечення держави та суспільства; життєво важливі функції та/або послуги; національна система захисту; суб'єкти й об'єкти захисту; функції держави; негативні наслідки; надзвичайні ситуації