Kuznichenko Sergii Oleksandrovich
doctor of legal sciences, professor, leading researcher of the Research Institute of Legal Support for Innovative Development of the National Academy of Legal Sciences of Ukraine
ORCID: 0000-0002-9278-2756

Batiuk Oleg Volodymirovich
doctor of Law, Professor of the Department of State Security of the Volyn National University named after Lesya Ukrainka
ORCID: 0000-0002-2291-4247

REGARDING THE FORMATION OF THE CONCEPT OF CRITICAL INFRASTRUCTURE PROTECTION: THE EXPERIENCE OF THE COUNTRIES OF THE EUROPEAN UNION AND THE USA

The need for a systematic approach to the protection of objects and resources critically important for the functioning of society and ensuring national safety is substantiated. The experience of the USA and the countries of the European Union regarding the protection of critical infrastructure is analyzed. The essence of the concept of "critical infrastructure" is considered. It is proposed to update the concept of critical infrastructure protection taking into account Industry 4.0 technologies.

Keywords: critical infrastructure, protection of critical infrastructure, national safety, USA, European Union, Industry 4.0 technologies.

The urgency of the topic is due to the fact that the reliable protection of critical infrastructure of the state is one of the priorities in providing the needs of national safety. Solving this problem needs a systematic approach at the national level. The global trends of increasing the threats of natural and manufactured nature, increasing the level of terrorist threats, increasing the number and increasing the complexity of cyber-attacks, as well as the damage to infrastructure facilities in the eastern and southern regions of Ukraine, as a result of the armed aggression by the russian federation, indicate the urgency of the problem for Ukraine. All this together leads to

the actualization of the issue of the protection of systems, facilities and resources, that are critically important for the functioning of society, social and economic development of the state and providing the national safety.

For the first time, scientific studies of critical infrastructure began in the 80s of the 20th century in the USA, when the National Research Council proposed a definition - critical infrastructure as a set of interconnected elements that support the integrity of the entire structure and primarily included major highways, roads, bridges, public transport networks, airports, water delivery and water sources, waste water and hazardous waste management, production and transmission of electricity and telecommunications [1, p.22-23]. The first scientific concept of critical infrastructure was first formed and developed in the USA, and this country is considered the first in developing and implementing the concept of critical infrastructure and its protection. After the serious terrorist attacks in September 2001, the president, parliament and government of the country revised not only their idea of the security system of the state and society under new geopolitical conditions, but also changed the national legislation, the structure of the government, the state budget, and the determination of priorities of the main directions of internal and external politicians.

In 2002in the USA, a corresponding document was adopted - the Critical Infrastructure Information Act ("CIIA") [2], which regulated the provisions on the exchange of information on the assessment of vulnerability and threats to infrastructure, including those related to terrorist threats The Act introduced the term "critical infrastructure information" to mean information that is not normally available to the public and is related to the security of critical infrastructure or protected systems. This Act designated a government agency, the Department of Homeland Security, to be responsible for collecting, analysis and dissemination of information in order to take the necessary measures to protect critical infrastructure. At the same time, the law established requirements for the use of such information (a limited access regime is introduced) to prevent abuse and protect business entities (infrastructure operators) from the dissemination of vulnerable commercial

information [3, c .153]. Since that time, the United States has continued to maintain its leadership position in this field, including through the use of modern management approaches proven in other areas, improvement of information and analytical support for the decision-making process, use of the latest technologies, and active dissemination of various forms and formats of personnel training and the public to ensure the protection and resilience of critical infrastructure. One example of this is the creation in 2018 in the system of the US Department of Homeland Security, the Agency for Cyber Security and Infrastructure Security, which functions as an operational component that at the national level manages efforts aimed at awareness and management of risks posed by threats to the country's critical infrastructure [4, p.4-5, p. 8].

Today, most of the developed countries of the world widely use the experience and useful developments in the protection of critical infrastructure, which were received and continue to be received by specialists from the USA. Since 2003, security research has been actively conducted at the international level within the framework of the international EU program "European industrial potential in the field of security research" and "European Security Research Programmed (ESRP)". Since 2007, many European countries have started work on the "Research for Secure Europe" initiative in order to prepare measures in case of war or emergency. Along with the above, since 2004, the creation of the European Program for Critical Infrastructure Protection ("EPCIP") project for the protection of critical infrastructure began at the level of the EU and the European Commission. In it, important attention was paid to protection against terrorist threats.

In Poland, the understanding of critical infrastructure is given in the Law of April 26, 2007 "On Crisis Management", on April 30, 2010, the Regulatory Act of the Council of Ministers (Government) of Poland "On the National Program for the Protection of Critical Infrastructure" was issued in Poland, in which § 3 responsibility for the development of criteria for the classification of objects into the system of critical infrastructure is assigned to the Director of the Government Center for Security [5]. In May 2020, the Republic of Poland adopted a new "National Security

Strategy of the Republic of Poland, 2020", which, as in many other countries, took into account new threats posed by pandemic cases and the latest developments related to the COVID-19 pandemic. In connection with the importance of timely and truthful information to the population about threats, prevention, measures to prevent diseases, separate objects, which are communication systems, have been named as an important element of the Polish national critical infrastructure.

In Germany, the main coordinator of critical infrastructure protection is the Federal Ministry of the Interior. The institution of the Protection of Critical Infrastructure in Germany (Schutz Kritischer Infrastrukturen in Deutschland) was also created, which investigates the vulnerability of infrastructure and proposes strategies for its protection and a policy of cooperation and cooperation of public administration with private actors.

In 1999in Great Britain, the National Infrastructure Security Coordination Center (NISCC) was created, which was first part of the Ministry of Internal Affairs, and then the Council of the National Security Advice Center (NSAC). Since 2007, these organizations have been replaced by the National Security Advice Center (NSAC). Great Britain, following the example of the USA, focuses primarily on terrorism and violations of cyberspace in the protection of critical infrastructure [1, p.39-40].

In France, the Prime Minister is responsible for coordinating the activities of the critical infrastructure sector, and in the organizational component, these functions are performed by the General Secretary for Defense and National Security (Secrétariat Généraldela Défenseetdela Sécurité Nationale - SGDSN), which is directly subordinate to the Prime Minister. From the point of view of legal support, the main document is the law on the protection of the main economic sectors of 2014 No. 6600/SGDSN/PSE/PSN (Secteursd'Activitésd'Importance Vitale), according to which all sectors serving to ensure the main social and economic processes, in particular, public administration, judiciary, armed forces, agriculture, electronic communication systems, energy, space and research, water, industry, public health, transport.

In the Slovak Republic, until 2011, the state's critical infrastructure was considered within the framework of defense infrastructure, and in 2011, Law No. 45/2011 "On Critical Infrastructure" was issued, according to which supervision over individual sectors is carried out by relevant ministries. At the same time, the Ministry of Internal Affairs acts as the main body for the protection of critical infrastructure [1, p.45-46, p.50].

The Directive of the European Commission No. 786 of 2006 included those objects of the national critical infrastructure of EU member states, the impact of which, in case of failure, incident or malicious intervention, will extend to the country where such an object is located, to the pan-European critical infrastructure. as well as to at least one other EU member country [6]. Another Council Directive 2008/114/EU of December 8, 2008 on the identification and determination of European critical infrastructures and the assessment of the need to improve their protection and protection introduced the procedure for the identification and determination of European critical infrastructures, as well as a common approach for European countries to assess the need for improvement protection of such infrastructures in order to contribute to the protection of people. "Critical infrastructure" for the purposes of this Directive means an object, system, or part thereof, located in the Member States, which is essential for the maintenance of vital public functions, health, safety, security, economic or social well-being of the population, the damage or destruction of which would have a significant impact in the Member State due to the inability of such infrastructure to support the mentioned functions. "European critical infrastructure" means critical infrastructure located in Member States, the damage or destruction of which would have a significant impact on at least two Member States. The significance of the impact is assessed using end-to-end criteria [7].

Today, the term "critical infrastructure" is included in the regulatory and legislative acts of many states, where its understanding is slightly different, but such differences are not significant. It is general that the term "critical infrastructure" usually covers those objects, systems, networks or their parts, the malfunctioning or

destruction of which will lead to the most serious consequences for the social and economic sphere of the state, will negatively affect the level of its defense capability and national security. In addition, the functioning of critical infrastructure in peacetime is associated with the maintenance of vital functions in society, the protection of the basic needs of its members and the formation of their inner sense of safety and security.

The implementation of state measures for the protection of critical infrastructure should take place in various spheres and directions, not only in legislative and criminal law. The experience of the USA and the EU proves the need to use the latest Industry 4.0 technologies in the system of ensuring the safety of infrastructure facilities, which should be reflected in the concept of critical infrastructure protection and relevant legislation.

ЛІТЕРАТУРА

1. Сметана М. Защита критической инфраструктуры: подходы государств Европейского Союза к определению элементов критической инфраструктуры. Острава: Czech Republic Development Cooperation. 2014/15. 60 с.

2. Critical Infrastructure Information Act of 2002 («CIIA»). URL: https://www.fas.org/sgp/crs/RL31762.pdf.

3. Курбанов Я. Л. Забезпечення природно-техногенної безпеки в Україні і проблема визначення поняття «критична інфраструктура». *Південноукраїнський правничий часопис*. 2-2016. С.150–154. URL: http://nbuv.gov.ua/UJRN/Pupch_2016_2_43.

4. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О.М. Суходолі. Київ: НІСД, 2020. 28 с.

5. Uchwała nr 121/2018 RadyMinistrów z dnia 7 września 2018 r. zmieniającejuchwałę w sprawieprzyjęcia Narodowego Programu Ochrony

Infrastruktury Krytycznej. URL: https://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf.

6. Бірюков Д.С. Про доцільність та особливості визначення критичної інфраструктури в Україні. Аналітична записка. 02.01.2013. URL: http://www.niss.gov.ua/articles/1026/.

7. Директива Ради 2008/114/ЄС від 8 грудня 2008 р. про ідентифікацію і визначення Європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. *Офіційний вісник Європейського Союзу*. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text.

REFERENCES

1. Smetana, M. (2014). *Critical infrastructure protection: approaches of the European Union states to determine the elements of critical infrastructure*. Ostrava: Czech Republic Development Cooperation. 2014/15 [in Russian].

2. Critical Infrastructure Information Act of 2002. Retrieved from: https://www.fas.org/sgp/crs/RL31762.pdf

3. Kurbanov, Ya. L. (2016). Ensuring natural technogenic safety in Ukraine and the problem of defining the concept of «critical infrastructure». *Pivdennoukrainskyi pravnychyi chasopys*, *2*, 150–154. Retrieved from: http://nbuv.gov.ua/UJRN/Pupch_2016_2_43 [in Ukrainian].

4. Sukhodol, O. M. (Ed.). (2020). *State Critical Infrastructure Protection System in National Security System*. Kyiv: NISD [in Ukrainian].

5. Uchwała nr 121/2018 RadyMinistrów z dnia 7 września 2018 r. zmieniającejuchwałę w sprawieprzyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej. Retrieved from: https://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf [in Polish].

6. Biriukov, D. S. (2013). On the expediency and peculiarities of determining critical infrastructure in Ukraine. 02.01.2013. Retrieved from: http://www.niss.gov.ua/articles/1026/.

7. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Retrieved from: https://zakon.rada.gov.ua/laws/show/984_002-08#Text [in Ukrainian].