https://nayka.com.ua/index.php/ee/article/view/661. DOI: http://doi.org/10.32702/2307-2105.2022.10.25

3. Буряк А.А. Інвестиційне співробітництво між Україною та ЄС у промисловості: регіональний розріз. *Науковий вісник Міжнародного гуманітарного університету. Серія: «Економіка і менеджмент*. 2017. № 25/2017. С. 49 – 53. http://reposit.pntu.edu.ua/handle/PoltNTU/1662.

UDC 338.246.8

Yevhenii Havlovskyi
applicant for the third (scientific) level of higher education
National University «Yuri Kondratyuk Poltava Polytechnic»

INSTITUTIONAL AND LEGAL PRINCIPLES OF SUPPORTING CRITICAL INFRASTRUCTURE ENTERPRISES IN THE EUROPEAN UNION COUNTRIES

Contemporary global transformations in the security environment caused by hybrid wars, cyber threats, energy crises, and technological advances necessitate strengthening the role of the state in ensuring the resilience of critical infrastructure. The countries of the European Union have developed a comprehensive institutional and legal model aimed at ensuring the continuity of strategically important enterprises that form the basis of economic, energy, food, transport, and information security. This model integrates legal norms, public administration tools, mechanisms for cross-sectoral cooperation, and partnerships between the state and the private sector, which increases the security system's adaptability to crisis challenges.

Research into the institutional and legal foundations for supporting critical infrastructure enterprises is particularly relevant in the context of military operations on the territory of Ukraine, when not only national security but also the stability of the state's integration into the European security and economic space depends on the effective management of critical assets. An analysis of the experience of EU countries makes it possible to identify key areas for the formation of an adaptive policy of state support for critical infrastructure, consistent with the principles of strategic autonomy, energy independence, and digital resilience.

The institutional and legal system for supporting critical infrastructure enterprises in European Union countries is multi-level and based on the principles of proportionality, subsidiarity, resilience, and integrated risk management. The central document defining the EU's policy framework for critical infrastructure protection is Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive), adopted in December 2022 [1]. It replaced the previous Directive 2008/114/EC and established an expanded list of critical infrastructure sectors,

including energy, transport, water supply, healthcare, digital services, and public administration.

An important institutional framework is the European Commission's Directorate-General for Civil Protection and Humanitarian Aid (DG ECHO), which coordinates the implementation of EU policy in the field of crisis prevention, emergency response, and support for the functioning of critical infrastructure in the event of emergency threats [2]. It oversees the EU Civil Protection Mechanism (UCPM), which ensures coordination between Member States in the event of threats to cyber infrastructure, energy networks, or transport systems.

The European Union Agency for Cybersecurity (ENISA) plays a key role in the digital dimension of security, implementing the NIS2 Directive (Network and Information Systems Directive, 2023), which aims to strengthen the cyber resilience of critical digital infrastructure companies, such as energy suppliers, financial institutions, transport operators, and telecommunications companies. This document requires member states to develop national cybersecurity strategies, certification systems, and mandatory monitoring of cyber incidents.

EU countries are actively implementing the “Resilience by Design” approach, which involves integrating security requirements into all stages of the life cycle of critical infrastructure systems – from design to operation [3]. Within this paradigm, a partnership is being formed between state regulators, the private sector, and research institutions. Financial support for such entities is provided by special EU programs, in particular Horizon Europe (Cluster 3 – Civil Security for Society), the Digital Europe Program, and the Connecting Europe Facility (CEF). These mechanisms are aimed at financing projects to improve cyber and energy resilience, develop smart grids, and introduce early warning systems [4].

Thus, the institutional and legal framework for supporting critical infrastructure enterprises in the EU is characterized by its systematic, multi-level, and flexible nature. They combine regulatory instruments (directives, regulations, strategies), organizational and institutional structures (agencies, coordination centers, partnership networks), and financial and economic instruments. For Ukraine, which is seeking integration into the European security space, it is advisable to adapt these approaches by creating a national model for supporting critical infrastructure enterprises based on the principles of institutional interaction, digital resilience, and legal compliance with EU standards.

References

1. European Commission. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (CER Directive). Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557

2. DG ECHO. (2023). Union Civil Protection Mechanism Annual Report 2023. Brussels: European Commission. URL: https://civil-protection-humanitarian-aid.ec.europa.eu

3. National Cyber Security Centre (NCSC, UK). (2023). Resilience by Design: Policy Principles for Critical Infrastructure. London: UK Government. URL: https://www.ncsc.gov.uk

4. OECD. (2023). Strengthening Critical Infrastructure Resilience: Policy Toolkit. Paris: OECD Publishing. URL: https://infrastructure-toolkit.oecd.org/governance/strengthen-critical-infrastructure-resilience/

UDC 331.108.45:330.131.7(477)

Oleksandr Gaydash
applicant for the third (scientific) level of higher education
National University «Yuri Kondratyuk Poltava Polytechnic»

PERSONNEL SECURITY OF UKRAINIAN ENTERPRISES IN THE CONDITIONS OF GLOBAL CHALLENGES AND THREATS

The modern economic system operates in conditions of unprecedented global transformations, which lead to increased uncertainty and risks in the socio-economic environment. For Ukrainian enterprises, which are simultaneously affected by military action, economic turbulence, technological changes, and demographic imbalances, ensuring personnel security as a key factor in economic stability and competitiveness is of particular importance.

Personnel security is a system-forming element of an enterprise's economic security, as it is the human resources that ensure the continuity of production processes, innovative capacity, adaptability to changes in the external environment, and the implementation of strategic goals. In the face of global challenges – such as the digitalization of the economy, mass migration of labor resources, a shortage of highly qualified personnel, and the growth of cyber threats and hybrid risks – the personnel management system needs to be rethought from the perspective of a risk-oriented approach and the formation of an institutional culture of occupational safety and loyalty.

For Ukraine, personnel security has two dimensions: on the one hand, it is the protection of human resources from losses, demotivation, and brain drain; on the other hand, it is the development of strategic competencies capable of ensuring economic recovery in the post-war period. Therefore, researching the issue of human resource security in the context of global challenges and threats is not only scientifically sound but also practically necessary for the formation of effective human resource risk management policies, increasing business resilience, and developing human capital as the basis for national competitiveness.

According to analytical data from the State Statistics Service of Ukraine, in 2022–2023, the number of employed people dropped by almost 2.8 million [1],