DOI: https://doi.org/10.30525/978-9934-26-352-1-22

## APPROACHES TO THE RISK MANAGEMENT SYSTEM IN THE FUNCTIONING OF ENERGY INFRASTRUCTURE

**Nataliia Trushkina**
*Ph.D. (in Economics), Senior Researcher,*
*Doctoral Candidate, Senior Research Officer*
*of the Sector of Industrial Policy and Innovative Development*
*of the Department of Industrial Policy and Energy Security,*
*Research Center for Industrial Problems of Development*
*of the NAS of Ukraine*
*Kharkiv, Ukraine*

Currently, ensuring the security of critical energy infrastructure [1] requires a shared understanding of all existing requirements, as well as the vulnerabilities of all components affecting the energy supply chain. One of the methods for solving these issues is the formation of a risk management system.

The risk management system is designed to identify and eliminate vulnerabilities in the energy sector as a critical element of critical infrastructure [2–4]. It should provide responsible parties in the energy sector with a standardized approach to quantifying and managing risks in the international supply of electricity. The risk management framework is based on an analysis of the measures already used by operators in the energy sector and member governments, as well as the actions that will be required in the future to close existing gaps in system security. In other words, this system sets a minimum standard, but can be adapted by individual States and operators according to their needs and characteristics.

The risk management system is designed to be as useful as possible to the maximum number of stakeholders. To achieve this, it has been made sufficiently flexible and allows each stakeholder to take into account the risks that exist in his or her own area of responsibility. For example, at the EU level, the main benefit of using this system is risk management in international electricity supplies. At Member State level, the network operator may need to perform risk management across other, not necessarily national, borders. This system can be used at each level, so before applying it, it is necessary to establish at which of the following levels it will be applied:

1) at a cross-border level within the EU (in cases where a functional failure in the ICT system leads to an interruption in the energy supply from one State Party to another Party State, or when the disrupted flow of energy is in transit through a Party State towards its final destination);

2) at a cross-border level outside the EU (in cases where a functional failure in the ICT system in a non-EU country affects the energy supply to a member state);

3) at the national level of a State Party (in cases where a functional failure in the ICT system in one part of a country's national infrastructure affects the energy supply to a significant part of the population within one State Party);

4) at the inter-organizational level (in cases where a functional failure in the ICT system in one organization affects the activities of another organization as a result of a power failure within one participating state);

5) at the intra-organizational level (in cases where a functional failure in the ICT system of one energy company leads to an interruption in the supply of energy within the member state in which this company is located).

The general approach to risk management developed by the International Risk Governance Council (IRGC) is based on a template structure for the process. This template breaks down the activities within the process into five elements: preliminary assessment to obtain an overview of the risk; assessment to determine the knowledge needed to make judgments and decisions; identification and analysis to assess risk acceptability; governance to define the roles of process participants; communication to develop an information exchange process (as explained in a study by the European Commission, the energy risk management system includes four steps: preliminary assessment; assessment; definition and analysis; management. At each step, it reminds users to consider the fifth element, communication. These steps can be repeated to provide a basis for continuous improvement). In addition, the framework recommends that each country and organization designate an expert responsible for implementing the risk management system and achieving its objectives to address identified vulnerabilities.

When implementing a risk management system, the aspect related to public-private partnerships should be considered. In September 2010, the Anti-Terrorism Unit of the OSCE Secretariat published a thematic overview summarizing key recommendations for critical energy infrastructure. These recommendations were developed at a seminar of public-private experts “Protecting Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks” held under the auspices of the OSCE. The OSCE emphasizes that these recommendations do not always imply agreement by all OSCE

participating States or the OSCE Secretariat with the proposed measures. Key recommendations include the following:

1) Follow a comprehensive approach based on risk assessment. Measures to protect energy infrastructure must be dynamic and based on a current and regularly updated assessment of all hazards.

2) Expand the scope of multi-stakeholder cooperation (an integrated approach to protecting critical energy infrastructure, as outlined above, involves the coordinated participation of multiple stakeholders representing various government agencies, the public and private sectors, and foreign stakeholders).

3) Develop flexible security measures that guarantee protection at the minimum appropriate level (the vulnerabilities and risk environment of each critical energy infrastructure facility are specific and dynamic; they must be taken into account when providing security to ensure that protection is cost-effective and consistent with the identified risks).

4) Increase focus on preparedness and overall resilience (preparedness requires advance contingency planning, testing and monitoring, including the development of communication plans with the public/customers and energy markets. To ensure greater resilience, increased investment in interconnectivity and alternative supply routes, as well as increasing storage capacity/strategic stocks).

5) Identify and eliminate the vulnerabilities of the energy sector in cyberspace (in today's increasingly computerized and ICT-dependent world [5], traditional physical security measures ("arming, fencing and security") are no longer sufficient. It is necessary to significantly improve the level of public and corporate awareness and understanding of cybersecurity issues, and the development of specialized cybersecurity skills should be encouraged).

6) Develop effective public-private partnerships [6-7] (it is necessary to clearly define the roles and responsibilities of stakeholders in the private sector and public authorities in the field of security. Partnerships can be developed for the purpose of jointly assessing the safety of critical energy infrastructure facilities, reviewing safety measures, developing emergency plans and incident response preparations).

7) Strengthen cross-border and international cooperation (the consequences of a failure in one energy infrastructure complex can extend far beyond the national borders of the country where it is located, be it a loss of supply or other damage, including economic (for example, rising prices in unstable energy markets) or environmental. Countries should carefully consider these direct and indirect dependencies, which will lead to a legitimate

interest in cooperation to ensure the integrity of the energy infrastructure. Several other countries and organizations have developed their own risk management systems. For example, the risk management system is an integral part of the US NIPP).

To summarize, we can say that energy systems are becoming more and more complex, and therefore more and more susceptible to disruptions. The protection of critical infrastructure in general and the interconnection of critical infrastructure and ICT systems are of particular importance to both public authorities and private sector companies.

Overall, it is important to remember that cybersecurity is increasingly vulnerable, and awareness of potential threats, as well as preparedness to counter them, are becoming increasingly important. The introduction of a risk management system provides a unified method for identifying and eliminating vulnerabilities in the functioning of energy infrastructure.

**References:**

1. Trushkina, N., Pahlevanzade, A., Pahlevanzade, A., & Maslennikov, Ye. (2021). Conceptual provisions of the transformation of the national energy system of Ukraine in the context of the European Green Deal. *Polityka Energetyczna – Energy Policy Journal*, *24*(4), 121–138. DOI: https://doi.org/10.33223/epj/144861

2. Kyzym, M. O., Khaustova, V. E., & Trushkina, N. V. (2022). Sutnist poniattia «krytychna infrastruktura» z pozytsii natsionalnoi bezpeky Ukrainy [The essence of the concept of "critical infrastructure" from the standpoint of national security of Ukraine]. *Biznes Inform – Business Inform*, *12*, 58–78. DOI: https://doi.org/10.32983/2222-4459-2022-12-58-78 [in Ukrainian].

3. Khaustova, V., Tirlea, M. R., Dandara, L., Trushkina, N., & Birca, I. (2023). Development of Critical Infrastructure from the Point of View of Information Security. *UNIVERS STRATEGIC – Revistă de Studii Strategice Interdisciplinare și de Securitate*, *1*(53), XIV, 170–188.

4. Bezpartochnyi, M., Trushkina, N., & Birca, I. (2023). Critical infrastructure development management mechanism: theoretical aspects. *Current issues of the management of socio-economic systems in terms of globalization challenges*: scientific monograph (pp. 612–628). Košice: Vysoká škola bezpečnostného manažérstva v Košiciach. https://doi.org/10.5281/zenodo.7799542

5. Kwilinski, A., Hnatyshyn, L., Prokopyshyn, O., & Trushkina, N. (2022). Managing the Logistic Activities of Agricultural Enterprises under Conditions of Digital Economy. *Virtual Economics*, *5*(2), 43–70. DOI: https://doi.org/10.34021/ ve.2022.05.02(3)

6. Khaustova, V., Zhukova, I., & Trushkina, N. (2023). Zakordonnyi dosvid finansovoho zabezpechennia vidbudovy ta modernizatsii krytychnoi infrastruktury [Foreign experience of financial support for reconstruction and modernization of critical infrastructure]. *Věda a perspektivy*, *7*(26), 178–192. DOI: https://doi.org/10.52058/2695-1592-2023-7(26)-178-192 [in Ukrainian].

7. Trushkina, N., & Zhukova, I. (2023). Derzhavno-pryvatne partnerstvo yak kliuchovyi pryntsyp funktsionuvannia natsionalnoi systemy zakhystu krytychnoi infrastruktury v Ukraini [Public-private partnership as a key principle of functioning of the national critical infrastructure protection system in Ukraine]. *Naukovi innovatsii ta peredovi tekhnolohii – Scientific innovations and advanced technologies*, *7*(21), 11–26. DOI: https://doi.org/10.52058/2786-5274-2023-7(21)-11-26 [in Ukrainian].