

Kiporenko O.V.

APPROACHES TO RISK MANAGEMENT OF ENERGY ENTERPRISES

In the current conditions of development and maintenance of the national economy at a sufficient level to meet the needs of producers and consumers, energy resources play a key role. The sustainability of energy companies is possible only if security is maintained at all stages of the company's life cycle, i.e. during design, operation, modernisation, work beyond the project timeframe, and decommissioning (mothballing) of equipment and facilities. The security of an energy company involves assessing the consequences of threats and their impact on the continuity of fuel and energy supply for consumers (population, business, state and society), as well as analysing the ability of energy security actors to prevent the development of negative scenarios[1].

To ensure a comprehensive approach to security, as required by energy sector regulations, it is necessary to develop a strategy for diagnosing, monitoring, identifying and forecasting possible threats, which can be done through risk analysis and risk management.

Risk management is a globally recognised comprehensive approach that involves the development of appropriate targeted measures and their inclusion in state planning documents. The ultimate goal is to prevent the emergence of new risks and reduce the known risks of negative developments by implementing comprehensive measures at the facility, industry and national levels.

It should be noted that there are different approaches to risk assessment. A generalised approach to risk assessment includes[2]

- Identification of threats, assessment of the frequency (probability) of each threat;
- assessment of vulnerability to each threat, which, taking into account its frequency
- determines the likelihood of damage;
- assessing the consequences (damage) for the worst-case scenario.

Risk-based approaches are widely used in the world's leading countries. For example, in 2015, the EU approved the Risk Assessment Methods for Critical Infrastructure Protection. Part II. A New Approach [3]. This document is based on the analysis of threats and risks. In addition, in the EU countries, it is recommended to use a risk matrix for the purpose of National Risk Assessment, depending on the relative impact of certain threats (Relative Impact) and their probability (Relative Likelihood). This document is based on the analysis of threats and risks. In addition, in EU countries, it is recommended to use a risk matrix for the purpose of National Risk Assessment, depending on the relative impact of the identified threats (Relative Impact) and their probability (Relative Likelihood).

Risk analysis in leading countries has become an important element in the national security system.

National risk assessment, which ensures the implementation of a number of important elements of the national resilience system, namely

- Foresight (risk identification) - a broad search for information is carried out to determine where a problem may arise and what potential threats exist;
- Risk register - identification of the most probable threats, the realisation of which may cause the most severe consequences for the country in the next five years (based on the analysis of information, analytical and scientific judgements and intelligence on the probability and consequences of the realisation of threats);
- risk assessment - the actual formation of an understanding of the complex of risks that the national security system should be set up to prevent, which forms the overall national risk assessment.

The generalised experience of risk management is reflected in the international standard IEC/ISO 31010:2009 Risk management - Risk assessment techniques and the corresponding national standard of Ukraine DSTU IEC/ISO 31010:2011[4, 5]. This standard is also useful because it describes almost all the methods used in risk analysis in a sufficiently complete manner. It should be noted that, depending on the entities targeted by energy security activities, these activities have some differences, since with regard to facilities, they are primarily aimed at reducing the level of threats and vulnerability of facilities, minimising the consequences, and with regard to processes and functions, at the continuity of their provision and rapid recovery in case of interruption. In this regard, modern crisis management technologies based on a business continuity management system can be useful.

References:

1. Energy Security of Ukraine: Methodology of System Analysis and Strategic Planning: Analytical Supplement / [Sukhodolya O. M., Kharazishvili Y. M., Bobro D. H., Smenkovskyi A. Y., Riabtsev H. L., Zavhorodnia S. P.] ; edited by O. M. Sukhodolya - Kyiv : NISS, 2020. 178 p.
2. Approaches to assessing the risks of functioning of systems of objects for various purposes. Mechanical engineering: Collection of scientific papers. 2022. №29. C. 70 -79. DOI 10.32820/2079-1747-2022-29-70-79
3. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. URL: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/risk-assessment-methodologies-critical-infrastructure-protection-part-ii-new-approach>
4. IEC/ISO 31010:2019. Risk management - Risk assessment techniques. URL: <https://www.iso.org/standard/72140.html> .
5. DSTU IEC/ISO 31010:2013. Risk management. Methods for generic risk assessment. URL: <http://khoda.gov.ua/image/catalog/files/dstu%2031010.pdf>

Робота виконана під керівництвом доцента кафедри АМЕТ Грінченко Г.С.