DOI: https://doi.org/10.53486/dri2024.41
UDC: [330.131.7:338.49]:005.59(477)

RISK-ORIENTED APPROACH TO MANAGING THE CRITICAL INFRASTRUCTURE DEVELOPMENT IN COUNTRIES OF THE WORLD

Viktoriia KHAUSTOVA[54], Doctor of Economic Sciences, Professor
Nataliia TRUSHKINA[55], PhD in Economics, Senior Researcher

ORCID: https://orcid.org/0000-0002-5895-9287
ORCID: https://orcid.org/0009-0007-4093-6697

Abstract: *The changing, dynamic and unpredictable development of the external institutional environment, crisis phenomena, natural disasters, cyberattacks and wars, armed conflicts and active hostilities are the reasons for the emergence of various types of risks to the functioning and activity of critical infrastructure facilities in various countries of the world.*
In this regard, the issue of forming a risk management system is currently being updated with the aim of finding a fundamentally new toolkit and methods of risk assessment, management approaches to their levelling and minimization. All this requires an in-depth analysis of the essence and content of the risk-oriented approach in order to understand the dynamic laws of managing the development of critical infrastructure.
The article summarizes and systematizes the existing approaches to defining the meaning of the concept of "risk management". The author's interpretation of the terms "risk" and "risk management" from the standpoint of critical infrastructure development is provided.
It is proposed to consider the risk as a situation of uncertainty, possible danger that is perceived and accepted by critical infrastructure objects, which arises as a result of changes in the relevant production, marketing, innovation, technological processes and is evaluated by the probability of loss of profitability, damage, destruction, threat of protection and security. Risk management refers to the modern paradigm of anti-crisis management of the development of critical infrastructure, taking into account the consequences of crisis phenomena, emergency situations and armed conflicts.
As a result of the study, the relationship between risk, threats, risk-oriented approach, risk management and development of critical infrastructure using a bibliometric approach was revealed. The expediency of applying a risk-oriented approach to managing the development of critical infrastructure in Ukraine, taking into account the best world practices, is substantiated. The implementation of this approach will make it possible to systematically diagnose and assess the risks caused by the conditions of war, with the aim of forming an adaptively oriented management system for the development of critical infrastructure facilities on the basis of risk management, which will contribute to the implementation of successive changes in the organizational and resource provision of their security activities with taking into account the threats and challenges of the war and post-war periods.

Key words: *national economy, critical infrastructure, risk, development management, risk-oriented approach, risk management.*

JEL: D 81, H 54, H 56.

1. Introduction.

An effective national strategy for the protection of critical infrastructure facilities should be based on the concept of risk management and crisis management. Regardless of the institutional model chosen,

[54] v.khaust@gmail.com, Research Center for Industrial Problems of Development of the NAS of Ukraine (Kharkiv, Ukraine);
[55] nata_tru@ukr.net, Research Center for Industrial Problems of Development of the NAS of Ukraine (Kharkiv, Ukraine).

stakeholders involved in the protection of critical infrastructure should be familiar with these concepts and consistently apply them in their respective sector and areas of competence. This is also due to the fact that critical infrastructure facilities in countries around the world are exposed to real or potential threats and risks created by natural disasters, environmental and man-made disasters, terrorist attacks, cyberattacks and information wars, military conflicts (V. Khaustova et al., 2023a).
In view of this, the need for theoretical and methodological substantiation of the expedient use of a risk-oriented approach to managing the development of critical infrastructure and the development of appropriate mechanisms for its effective functioning in the risk management system determine the conduct of further research in this direction.

2. Basic content.
Risk is an abstract and complex concept. In general, risk can be defined as the impact of uncertainty on goals. According to other approaches, risk is defined as the combination of the probability of an event and the extent of damage it can cause, or as the combination of the probability and impact of any event. The terms „threat", „vulnerability" and „risk" are often confused, sometimes even used as synonyms. However, ensuring compliance with risk management standards requires a clear understanding of the difference between these terms, which can be difficult due to differences in standards. Therefore, it is important to adopt one definition and use it consistently.
Critical analysis of foreign scientific sources (J. Arlinghaus et al. (2021); T. Andersen et al. (2010); K. Cormican (2014); M. Crouhy et al. (2014); L. Haar et al. (2021)) shows that today there is no single theoretical approach to defining the essence of risk management. This is due to the fact that scientists are representatives of various economic theories and schools with their own scientific approaches and features, as well as the ambiguity and multifacetedness of this concept. After all, the term „risk management" is considered as an object of research from the standpoint of public administration, economic and financial security, insurance, investment, financial, strategic, marketing, and logistics management. Therefore, many scientific works indicate the interest of researchers in studying various aspects of risk management.
On the basis of theoretical analysis, it was established that researchers mostly understand the concept of „risk management" as science; methodology; art; process; system; structural components of the system; factor; managerial paradigm; a specific branch of management; a set of methods, techniques and measures.
So, based on the generalization of conceptual approaches to the definition of the concepts of „risk" and „risk-management", the author's interpretation of their content is proposed. Under risk, it is proposed to understand a situation of uncertainty, possible danger, perceived and accepted by critical infrastructure objects, which arises as a result of changes in the relevant production, marketing, innovation, technological processes and is evaluated by the probability of loss of profitability, damage, destruction, threat of protection and security. The term ‚risk management" is proposed to be considered as a modern paradigm of anti-crisis management of the development of critical infrastructure, taking into account the consequences of crisis phenomena, emergency situations and armed conflicts.
Using bibliometric analysis, it was established that the international scientometric database Scopus contains 495 publications that contain the words „Risk" and „Threats" and „Critical Infrastructure

Development". The scientific works of such scientists as A. Gheorghe (2004); X. Zhang (2005); P. F. Katina, et al. (2016); Yes. Brezhnev (2019); A. Fekete (2019); A. Fekete & J. Rhyner (2020); O. Korystin et al. (2022). As a result of the search, keywords related to the risk-oriented approach to managing the development of critical infrastructure were revealed. These words include: Risk Assessment (153 documents), Critical Infrastructures (103), Risk Management (72), Cybersecurity (65), Network Security (58), Security of Data (45), Risk Analysis (37), Computer Crime (30), Security Systems (29), Security (29), Risk Perception (29), Resilience (29), Vulnerability (28), Sustainable Development (28), Terrorism (23), Safety Engineering (21), Cyber-attacks (21), Climate Change (21), Risk (19), National Security (17), Hazards (16), Disasters (16), Threat (10 documents) and others. This is confirmed by the results of the bibliographic data analysis using the VOSviewer software (Fig.).

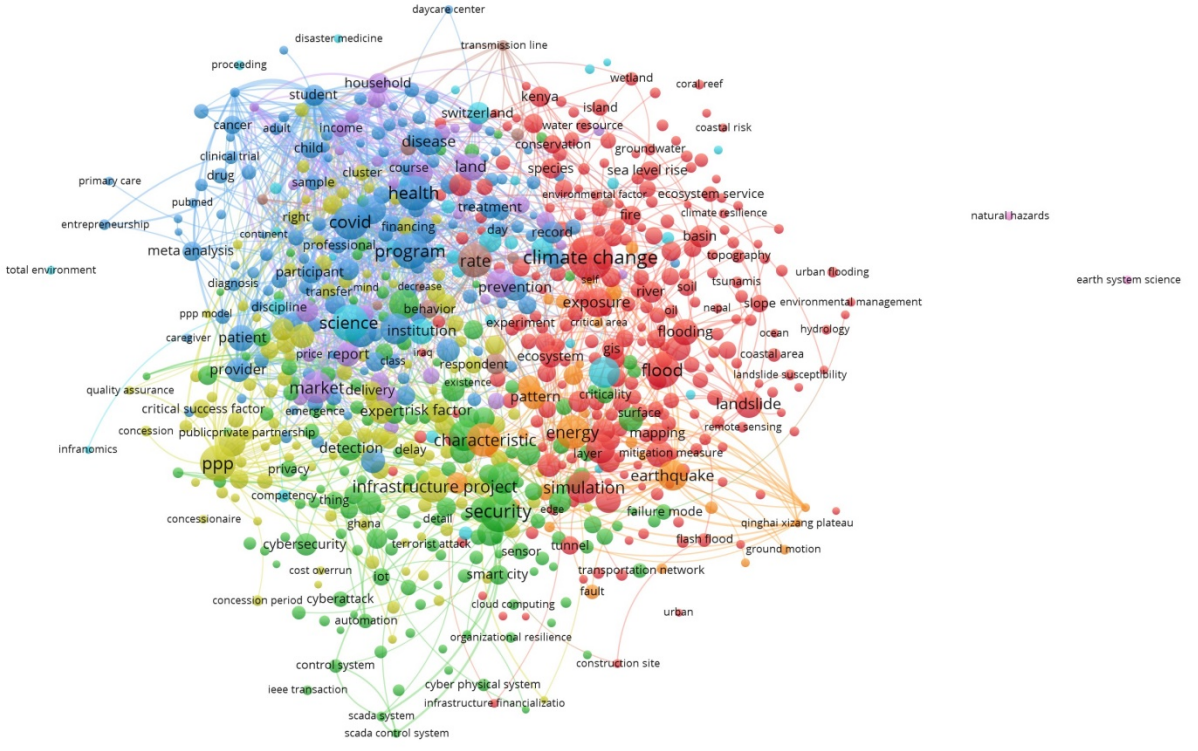

Figure. Network visualization of citations of articles on risk-oriented approach to managing the development of critical infrastructure, implemented using the VOSviewer toolkit

Source: built on the basis of the international scientometric database Scopus.

Various principles and measures are necessary for effective risk management of the organization. In order to apply a structured approach to risk management, it is necessary to combine all the necessary aspects and describe them within the framework of one comprehensive system designed to help organizations effectively manage risks. The individual structure of the risk management system depends on the size of the organization and the complexity of the organizational structure, its propensity to risk, legal regulations, as well as on the already existing elements of risk management or management systems.

The United Nations Office for Disaster Risk Reduction (UNISDR) defines risk management as a systematic approach and practice of managing uncertainty to minimize potential damage and loss.

Risk management involves assessing and analyzing risks, and implementing strategies and specific actions to control, reduce and transfer risks.

In the context of risk management processes as they relate to critical infrastructure protection, it is important to have a clear understanding of key concepts that are often used interchangeably, namely:

- Threat: anything that exploits a vulnerability of critical infrastructure;
- Vulnerability: a weakness in critical infrastructure that can be exploited by a threat;
- Risk: the probability of damage, injury, destruction or interference with the ability of critical infrastructure to provide its services as a result of a vulnerability exploited by a threat.

There is no unique or universal standard for risk management across the world. The use of different "authorities" by different stakeholders responsible for this task can lead to inconsistent results. At the national level, the use of different methodologies can make it difficult, if not impossible, to compare results within and across sectors, potentially impacting the reliability of operations as a whole. It is therefore important for countries to support the establishment of risk management processes that cover, at a minimum, the following elements:

- Establishing the context – the scope and parameters of the risk assessment;
- Risk assessment (definition, analysis, evaluation) – transforming risk data into information for decision-making;
- Risk mitigation – transforming risk information into decisions and actions to reduce risk;
- Communication and consultation – defining the methods of communication used by all stakeholders involved in the process;
- Monitoring and review – conducting regular reviews or oversight to improve risk management, identify changes in the context of existing risks and identify new risks.

To ensure that appropriate preventive security measures are identified, the risk management system should detail the mechanisms for obtaining reliable threat information and conducting risk assessments, taking into account international, national and regional situations and conditions. Security measures and procedures must be flexible and proportionate to the risk assessment, which may fluctuate depending on various changing factors. This system must be implemented in a timely and effective manner so that the resulting risk assessment is always up-to-date, accurate and complete.

Internationally, ISO has created a recognized paradigm in this area with the ISO 31000 standard. This belongs to a family of standards that ISO defines as a set of components that provide a framework and organizational mechanisms for developing, implementing and monitoring, reviewing and continually improving risk management throughout an organization. Taking the same approach to risk management as ISO 31000, the ISO 27000 series provides a reference standard in the field of information security systems. ISO 27000 thus offers a useful guidance framework for protecting critical information infrastructures. It is important to note, however, that ISO 31000 is not industry or sector specific.

Some countries, notably the United States and Canada, have created government programs specifically to encourage critical infrastructure operators to adopt a common assessment framework. These programs are also designed to provide technical assistance in conducting assessments under a "soft approach" based on incentives and voluntary plans.

Consider the Canadian Regional Resilience Assessment Program (RRAP) as a comprehensive risk assessment program for owners and operators of Canadian critical infrastructure. The program

includes site assessments to help organizations assess and improve their resilience to all hazards in Canada, such as cyber threats, accidental or intentional man-made events, and natural disasters. These on-site assessments are voluntary, non-regulatory, free, and confidential.

RRAP uses three primary tools to improve the resilience of critical infrastructure:

1) Critical Infrastructure Resilience Tool (CIRT): an on-site survey tool that measures a site's resilience and protective measures;

2) Critical Infrastructure Multimedia Tool (CIMT): a multi-platform software tool that generates an interactive visual guide to a critical infrastructure asset, featuring a spherical photograph;

3) Canadian Cyber Resilience Review (CCRR): an on-site survey tool that measures an organization's cybersecurity posture.

The program may include workshops, meetings, geospatial products, and subject-matter expert interviews. The results of RRAP assessments are designed to help owners and operators identify dependencies and vulnerabilities within their organizations. On-site assessments also identify a number of optional, cost-effective actions to help owners and operators reduce risks and improve their ability to respond to and recover from disruptions.

Specifically, RRAP provides for: improved risk management (increases an organization understands of its vulnerabilities through the use of robust assessment tools); strengthened government relationships; strengthened relationships with multiple government departments, including response agencies; increased cybersecurity awareness (better understanding how well an organization is prepared for cyber-attacks and other cyber threats). Other key factors for critical infrastructure owners and operators include: minimal time and resource investment (RRAP is a fast and free service); security (Public Safety Canada will protect the confidentiality of documents and information provided in confidence by critical infrastructure owners and operators to the department).

Taking Sweden as an example, it can be noted that, according to national legislation, all public authorities are required to develop and submit a risk and vulnerability analysis to the National Contingencies Agency (MSB). Based on such reports, the MSB has been producing national risk assessments since 2011. These documents (the most recent of which was released in 2016) are intended to provide a strategic basis for the direction and further development of civil contingencies. The 2016 assessment identifies five development areas that the MSB considers particularly important for improving disaster preparedness (and thus are of particular relevance to the protection of critical infrastructure): efforts in the field of disaster preparedness and civil defence should be given higher priority by responsible stakeholders in Sweden; knowledge and awareness of roles and responsibilities related to disaster preparedness must be increased, in particular when it comes to responsibility for geographical areas; risk and vulnerability analysis conducted at local, regional and national levels require improvements so that they can be used as a basis for disaster preparedness and civil defence planning; the scenarios provided by the MSB can become a supporting tool for disaster planning and development; clearer requirements for protective measures for critical infrastructures need to be established.

The MSB highlights the need to further develop capabilities in the following areas: Ability to respond to power outages; Ability to prevent and respond to interruptions in the supply of drinking water; Information and cybersecurity; Ability to prevent and respond to interruptions in the supply of medicines; Ability to prevent and respond to radiological and nuclear events.

Crisis management defines the processes that need to be activated when threats do materialize. The stages of crisis management include: crisis identification; planning an appropriate response to a crisis; Confronting and resolving a crisis.

When it comes to crisis management terminology, countries sometimes refer to "contingency plans" and "emergency plans" interchangeably. Strictly speaking, however, emergency plans are reactive in nature, while contingency plans are more proactive. While contingency plans are designed to limit the consequences or impact of an incident, contingency plans are designed to anticipate events and prepare all stakeholders for an emergency, as well as to ensure a prompt return to normal operations.

A single entity designated by the state should be given primary responsibility and authority for determining the course of action to be taken in the event of a crisis. This entity should coordinate all actions with all participating and affected entities. As part of the crisis management plan, an effective emergency response plan should be developed, including ensuring the interoperability of communication systems and adequate response times, as well as evacuation plans to limit the impact. The response of the emergency response team must be planned, tested and assessed in advance to mitigate the impact of an attack.

When developing their critical infrastructure protection strategies from a risk management perspective, countries should consider a number of guiding principles.

Determining the nature and levels of threats to critical infrastructure and the associated vulnerabilities is necessarily a collaborative and coordinated product of assessments conducted at multiple levels. However, a critical infrastructure protection strategy must be able to integrate multi-level threat, impact and vulnerability assessments. These levels are represented schematically as follows:

1) National level; 2) Sector level; 3) Infrastructure/company level.

The purpose of a national risk assessment is to provide an overview of the threat facing the country's critical infrastructure as a whole, its vulnerabilities and the consequences of a successful attack. An important contribution of national assessments is that they show how multiple sectors interact with each other. By developing documents of this type, recommendations and conclusions can be made based on the intelligence that has supported the development of national security and counter-terrorism strategies.

It is essential to develop sector-specific risk profiles for critical infrastructure. These profiles are critical to assessing existing mitigation practices, outcomes and vulnerabilities. Depending on the sector in question, risk assessments may be conducted for specific sub-sectors and subsequently fed back into broader sector risk profiles.

For example, Australia's Critical Infrastructure Resilience Strategy breaks down the transport sector into the following sub-sectors: aviation, land passenger transport (including bridges and tunnels), land freight and marine transport (shipping and ports).

According to the same strategy, the energy sector consists of electricity systems, offshore oil and gas fields, onshore oil and gas and coal supplies.

The assessment at the infrastructure level is that critical infrastructure operators are often the ones who know best how their infrastructure operates in terms of systems and processes. Consequently, they have a specific understanding of their internal vulnerabilities.

In addition, companies often conduct risk management cycles independently of the institutional role they are called upon to play in protecting critical infrastructure. Corporations primarily engage in risk

management to minimize damage that may impact the company's objectives in order to ensure business continuity or limit the impact of a threat. Without focusing on protecting critical infrastructure, this type of risk management aims to identify risks to business continuity and implement mitigation measures. As a result, this can directly benefit companies' infrastructures and enhance their resilience.

Therefore, countries should carefully consider the role that company-managed risk management processes should play in the context of critical infrastructure protection strategies. Ways to integrate corporate-level assessments into decision-making processes for the development of appropriate infrastructure support should also be included.

Consider the features of a risk-oriented approach to the management of energy infrastructure development (V. Khaustova et al., 2023b; 2024; A. Kwilinski et al., 2024; N. Trushkina, 2021; D. Wang et al., 2022). The energy infrastructure risk management system is designed to identify and eliminate vulnerabilities in the energy sector and ICT. It should provide responsible parties in the energy sector with a standardized approach to risk quantification and risk management during international electricity supplies. The risk management system is based on the analysis of the measures already used by operators in the energy sector and the governments of the Member States, as well as the actions that will be required in the future to eliminate existing gaps in the security of the system. In other words, it sets a minimum standard, but can be adapted by individual states and operators according to their needs and characteristics.

The risk management system is built in such a way as to be as useful as possible to the maximum number of interested parties. For this purpose, it is made quite flexible. It allows each interested person to take into account the risks that exist in their own area of responsibility. For example, at the EU level, the main advantage 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. The general approach to risk management developed by the International Risk Management Council (IRGC) is based on a template framework for this process. This template breaks down activities within the process into the following elements: 1) preliminary assessment of obtaining a general attitude to risk; 2) assessment of the definition of knowledge, necessary judgments and decisions; 3) definition and analysis to assess risk acceptability; 4) managing the definition of the roles of process participants; 5) communication of the development of the information exchange process.

As explained in the study of the European Commission, the risk management system in energy/ICT includes four stages: preliminary monitoring; assessment; definition and analysis; management. At each stage, it reminds users of the need to consider the fifth element – communication. These steps can be repeated to provide a basis for continuous improvement. In addition, within the framework of this system, each country and organization is recommended to appoint an expert responsible for the implementation of the risk management system and the implementation of its objectives for the elimination of identified vulnerable parties.

When implementing a risk management system, the aspect related to public-private partnerships should also be considered (M. Kyzym et al., 2023). In September 2010, the Anti-Terrorism Unit of the OSCE Secretariat published a thematic overview, which provides the main recommendations for the development of energy infrastructure facilities. These recommendations were developed at the

seminar of public-private experts "Protection of the most important objects of non-nuclear energy infrastructure from terrorist attacks" held under the auspices of the OSCE. Some main recommendations can be given: 1) adherence to an integrated approach based on risk assessment (energy infrastructure protection measures must be dynamic and based on an up-to-date and regularly updated assessment of all hazards); 2) expanding the framework of multilateral cooperation (a comprehensive approach to the protection of the most important energy infrastructure facilities involves the coordinated participation of numerous stakeholders representing various government bodies, the public and private sectors, as well as foreign stakeholders); 3) development of flexible security measures that guarantee protection at the minimum adequate level (vulnerable parties and the risk environment of each energy infrastructure facility have their own specifics and dynamics; they must be taken into account when providing security to ensure the cost-effectiveness of protection and its compliance with established risks); 4) paying more attention to ensuring preparedness and general stability (preparedness requires advance planning of actions in an emergency situation, testing and control, including the development of plans for informational interaction with the public - consumers and energy markets. To ensure the level of stability, it is necessary to increase the volume of investments in inter-network interaction and alternative supply routes, as well as storage capacity/strategic stocks); 5) identification and elimination of vulnerabilities of the energy sector in cyberspace (today, in a world increasingly computerized and dependent on ICT, traditional physical security measures are no longer sufficient. It is necessary to significantly increase the level of public and corporate awareness and understanding of cybersecurity issues, and the development of special skills in matters of cybersecurity should also be encouraged); 6) development of an effective public-private partnership (it is necessary to clearly define the roles and responsibilities of stakeholders in the private sector and public authorities in ensuring security. The partnership can be developed for the purpose of joint assessment of the security of the most important energy infrastructure facilities, review of measures security, development of action plans in emergency situations and preparation for response to incidents); 7) strengthening of cross-border and international cooperation (the consequences of a failure in the operation of one energy infrastructure complex can spread far beyond the state borders of the country where it is located, whether it is a supply interruption or other damage, including economic (for example, an increase in prices on unstable energy sales markets) or environmental (countries should carefully consider these direct and indirect dependencies, leading to a justified interest in cooperation to ensure the integrity of the energy infrastructure).

3. Conclusions.

At present, in the global world, multifaceted issues of the development of critical infrastructure in the conditions of the formation of a security environment have become especially relevant. Modern threats to national security and changes in the international security system must be taken into account by all countries of the world (and especially Ukraine) in their national policies and development strategies. Therefore, the development of Ukraine's critical infrastructure must be considered from the standpoint of ensuring national security and post-war economic development, taking into account world practice (the experience of South Korea, Japan, China, Germany, Great Britain, Bosnia and Herzegovina, Croatia, Poland, etc.).

In view of this, it is currently necessary to create a security environment as a basis for ensuring the protection and stability of critical infrastructure within the framework of the implementation of the measures of the National Plan for the Protection and Security and Stability of Critical Infrastructure, approved by the Order of the Cabinet of Ministers of Ukraine dated September 19, 2023 No. 825 -y., as well as the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated September 14, 2020 No. 392/2020.

For this, first, it is proposed to justify the feasibility of using a risk-oriented approach to managing the development of critical infrastructure:

identification of possible threats, risks, crisis situations and their systematization by different groups;

ranking of exogenous and endogenous factors influencing the development of critical infrastructure;

development of a comprehensive approach to risk management of critical infrastructure development in crisis situations;

development of the order or algorithm of actions for operational response to crisis situations and adaptation of the operation of critical infrastructure objects (especially in the field of energy) in the conditions of military operations;

development of recommendations on anti-crisis management of critical infrastructure development).

The implementation of a risk-oriented approach will make it possible to systematically diagnose and assess risks caused by the conditions of war, with the aim of forming an adaptive-oriented management system for the development of critical infrastructure facilities on the basis of risk management, which will contribute to the implementation of successive changes in the organizational and resource provision of their security activities taking into account the threats and challenges of the war and post-war periods.

In further studies, it is planned to justify and develop the Concept of the Nationwide target program for the post-war development of critical infrastructure within the framework of the implementation of the Recovery Plan of Ukraine.

Bibliographical references.

1. Arlinghaus, J. C., & Rosca, E. (2021). Assessing and mitigating the risk of digital manufacturing: Development and implementation of a digital risk management method. *IFAC-PapersOnLine*, *54(1)*, 337-342. https://doi.org/10.1016/j.ifacol.2021.08.159.
2. Andersen, T., & Schroder, P. (2010). Strategic risk management practice; How to deal effectively with major corporate exposures. Cambridge University Press, Cambridge.
3. Brezhniev, Ye. (2019). Multilevel Fuzzy Logic-Based Approach for Critical Energy Infrastructure's Cyber Resilience Assessment. In: *Proceedings of the 10th International Conference on Dependable Systems, Services and Technologies*, DESSERT 2019, 8770034, 213-217. https://doi.org/10.1109/DESSERT.2019.8770034.
4. Cormican, K. (2014). Integrated Enterprise Risk Management: From Process to Best Practice. *Modern Economy*, *5*, 401-413.
5. Crouhy, M., Galai, D., & Mark, R. (2014). The Essentials of Risk Management. 2nd ed. McGraw-Hill, New York, USA.
6. Fekete, A. (2019). Critical infrastructure and flood resilience: Cascading effects beyond water. *Wiley Interdisciplinary Reviews: Water*, *6(5)*, e1370. https://doi.org/10.1002/WAT2.1370.
7. Fekete, A., & Rhyner, J. (2020). Sustainable digital transformation of disaster risk – integrating new types of digital social vulnerability and interdependencies with critical infrastructure. *Sustainability (Switzerland)*, *12(22)*, 1-18, 9324. https://doi.org/10.3390/su12229324.

8. Gheorghe, A. V. (2004). Risks, vulnerability, sustainability and governance: A new landscape for critical infrastructures. *International Journal of Critical Infrastructures*, *1(1)*, 118-124. https://doi.org/10.1504/IJCIS.2004.003801.
9. Haar, L., & Gregoriou, A. (2021). Risk management and market conditions. *International Review of Financial Analysis*, *78*, 101959. https://doi.org/10.1016/j.irfa.2021.101959.
10. Hopkin, P. (2010). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page, London, UK.
11. Katina, P. F. et al. (2016). A Criticality-based Approach for the Analysis of Smart Grids. *Technology and Economics of Smart Grids and Sustainable Energy*, *1(11)*, 14. https://doi.org/10.1007/s40866-016-0013-2.
12. Khaustova, V., Trushkina, N., & Zinchenko, V. (2023a). Key challenges of restoring critical infrastructure of Ukraine in the conditions of post-war economic development. In: Khaustova, V. (ed.), *Post-war recovery of the economy of Ukraine: problems and solutions* (pp. 7-33). FOP Liburkina L.M., Kharkiv, Ukraine [in Ukrainian].
13. Khaustova, V., Hubarieva, I., Kostenko, D., Salashenko, T., & Mykhailenko, D. (2023b). Rationale for the Creation and Characteristics of the National High-Tech Production of Motor Biofuel. In: Zaporozhets, A. (eds.), *Systems, Decision and Control in Energy V. Studies in Systems, Decision and Control* (pp. 569-583), vol 481. Springer, Cham. https://doi.org/10.1007/978-3-031-35088-7_31.
14. Khaustova, V., Kyzym, M., Trushkina, N., & Khaustov, M. (2024). Digital transformation of energy infrastructure in the conditions of global changes: bibliometric analysis. In: *Proceedings of the 12th International Conference on Applied Innovations in IT* (Koethen, Germany, Match 7, 2024), *12(1)*, 135-142. Koethen: Anhalt University of Applied Sciences. http://dx.doi.org/10.25673/115664.
15. Korystin, O., Svyrydiuk, N., & Mitina, O. (2022). Risk Forecasting of Data Confidentiality Breach Using Linear Regression Algorithm. *International Journal of Computer Network and Information Security*, *14(4)*, 1-13. https://doi.org/10.5815/ijcnis.2022.04.01.
16. Kwilinski, A., Khaustova, V., & Trushkina, N. (2024). Transformation of the Energy Infrastructure in the Context of the Implementation of the European Green Deal. In: Babak, V., & A. Zaporozhets (eds.), *Systems, Decision and Control in Energy VI. Studies in Systems, Decision and Control* (pp. 59-79), vol. 561. Springer, Cham. https://doi.org/10.1007/978-3-031-68372-5_3.
17. Kyzym, M. O., Khaustova, V. Ye., & Trushkina, N. V. (2023). Financial Provision for the Development of Critical Infrastructure in the Context of Post-War Reconstruction of Ukraine's Economy. *Business Inform*, *8*, 263-274. https://doi.org/10.32983/2222-4459-2023-8-263-274.
18. 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. https://doi.org/ 10.33223/epj/144861.
19. Wang, D., Gryshova, I., Balian, A., Kyzym, M., Salashenko, T., Khaustova, V., & Davidyuk, O. (2022). Assessment of Power System Sustainability and Compromises between the Development Goals. *Sustainability*, *14(4)*, 2236. https:// doi.org/10.3390/su14042236.
20. Zhang, X. (2005). Critical success factors for public-private partnerships in infrastructure development. *Journal of Construction Engineering and Management*, *131(1)*, 3-14. https://doi.org/10.1061/(ASCE)0733-9364(2005)131:1(3).