НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«РЕЗИЛЬЄНТНІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ – 2023»

Збірник матеріалів конференції
21 червня 2023 р.

Київ – 2023

УДК 621.3 + 004 + 519.6 : 620.9

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол №4 від 25 травня 2023 р.)

Організаційний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Програмний комітет:
В.В. Мохор, В.О. Артемчук та ін.

Відповідальний за випуск:
В.О. Артемчук

Critical Infrastructure Resilience – 2023 : collection of materials of the scientific and practical conference, Kyiv, June 21, 2023, PIMEE of NAS of Ukraine. - 2023. - 109 p.

Резильєнтність критичної інфраструктури – 2023 : збірник матеріалів науково-практичної конференції, м. Київ, 21 червня 2023 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2023. – 109 с.

ЗМІСТ

M.V. Prazian

BUILDING CRITICAL INFRASTRUCTURE RESILIENCY: GHG INVENTORY AND DECARBONISATION PLAN MODELLING TO MOVE TOWARDS THE FINANCING STAGE

Building critical infrastructure resiliency requires more resources than usual due to energy, climate change, supply chain turbulence and inflation. By modest estimates Ukraine, for example, needs about 250 billion USD of foreign capital to fast the post-war recovery in five years (2023a). This number is a bit narrow compared with the need to tackle emergencies in the country and obtain sustainability and cyber-physical and digital resiliency for many critical infrastructures sectors: energy, water, food, industry, defence, ICT, transport, and others. It justifies a gigantic request for more scalable funds with a higher speed to invest them into the infrastructure.

The financial institutions can provide financial closes only under the project's cohesion with the European development aid and low-carbon and climate-resilient policies. The essential reference points for investment funds and banks in Eurozone are the Sustainable Finance Disclosure Regulation (SFDR) (2019) and the Guide on Climate-related and environmental risks published by the European Central Bank (ECB)(E. C. Bank, 2020). The Paris Agreement objectives and the Taskforce on Climate-related Financial Disclosures (TCFD) (2017) should align the projects. For most large and listed corporates, the Corporate Sustainability Reporting Directive (CSRD)(2022) and EU Taxonomy (2022) give a framework relating to climate mitigation and adaptation. A specific cohesion stage (E. I. Bank, 2023) precedes measures to assess projects as bankable because of their technical and economic feasibility. When the initial assessment fits the policy and requirements, the beneficiary can get the green light for the next steps, hoping to reach the financial close.

The beneficiaries developing critical infrastructure belong to sovereigns and sub-sovereigns, corporates, and special purpose vehicles (SPVs). The sub-sovereigns and sovereigns (governments) are direct signatories of the Paris Agreement and primarily perform as policymakers. The typical beneficiary of scientific and consulting services for the preceding stage can be a parent corporation that controls an entity, the SPVs, and often represents a group of companies and holdings. Their activity for increasing critical infrastructure resiliency has to follow the Science Based Target Initiative (SBTi)(WRI, 2023). The SBTi prescribes publicly disclosing mid-term (5 to 10 years) and long-term goals (up to 30 years). The plans cover the quantitative emission reduction targets, offsets' role, and the impact on stakeholders. The beneficiary used to be contractually obliged to work out the greenhouse gas (GHG) inventory and the decarbonisation plan with a commitment to a subsequent implementation of an environmental management system (ESM) according to ISO 14001(2023b).

GHG inventory of Scope 1, Scope 2, and Scope 3 collects all the data necessary under the GHG Protocol Corporate Standard developed by the World Resources Institute (WRI) and the World Business Council for Sustainable Development (WBCSD). It provides a framework for measuring and managing GHG emissions (2023d). The current GHG emissions inventory implies using secondary and tertiary data for benchmarking analysis with selected sources. A part of the primary data comes from its own supply chain and procurement disclosure upon request. Most corporates do not have relevant online systems for GHG data gathering representing a bottleneck and opportunity for innovation. Therefore, what is essential is that there is a space for implementing science and engineering. For instance, the R&D can obtain new-generation internet technologies, IoT, AI, ML, robotics, 5G/6G connectivity, blockchain, and data processing. Such technology prospects find a place in the content of the decarbonisation plans.

The decarbonisation plan (DP) justifies the ambition of quantitative emission targets for many years broken down into milestones. It explains long-term decarbonisation options, offsets' role, and stakeholder impact. Global leaders and responsible enterprises direct their plans to the public (eBooks.com, 2018). The regulators usually do not prescribe any specific format or structure for the document. Modelling the DP is a focal point where innovation, creativity, science, engineering, and regulation can have a decisive impact on strategic plans. The DP development is more down to models, including digital twins, methods, and prognosis concerning technology switch, energy efficiency, offsetting, cybersecurity, and standards. The resilience and sustainability of the entire supply chain, risks and impacts on the planet, people, profit, and non-financial externalities the ESG-like are objective. Academia, universities, and experts can help beneficiaries to identify and translate options into action plans. The author argues that multi-model methodologies can give the best results for target setting and its cost. The Science Based Targets Initiative (SBTi) is a good service tool in a raw.

The G.E. Pukhov Institute for Modelling in Energy Engineering of the National Academy of Science of Ukraine launched research in studying, assessing and ensuring the resilience of critical infrastructures in the electricity and other sectors(2023c). For example, Ukraine joined the European energy system ENTSO-E on 16 March 2022, which led to new necessities. Resiliency requires an effective policy where the GHG inventory and strategic and middle-term net-zero plans should be scientifically proven. Selecting a priority between energy, climate, supply chain (Prazian, 2023), and security is not always easy for stakeholders. Thus, academia, universities, professional associations, and experts will have a decent scope of work. The beneficiaries and intermediaries seek scientific advisory for capacity building and technical assistance. Before moving closer to the financial stage, where the bankable projects are ready for use, the beneficiaries must arrange their own scientifically based targets and documents as it becomes mandatory(Bui, 2023) in the EU in 2024.

1. Bank, E. C. (2020). *ECB publishes final guide on climate-related and environmental risks for banks*. https://www.bankingsupervision.europa.eu/press/pr/date/2020/html/ssm.pr201127~5642b6e68d.en.html
2. Bank, E. I. (2023). *The EIB Group PATH Framework: Supporting counterparties on their pathways to align with the Paris Agreement (Version 1.1)*. https://www.eib.org/en/publications/20220007-the-eib-group-path-framework
3. Bui, A. (2023, 8 June). *New EU Commission Sustainable Finance Package*. https://www.e3g.org/news/new-eu-commission-sustainable-finance-package/
4. eBooks.com. (2018). *Principles of Sustainable Finance*. EBooks.Com. https://www.ebooks.com/en-us/book/209554679/principles-of-sustainable-finance/dirk-schoenmaker/
5. EBRD. (2023a). *Ukraine needs $250 bln foreign capital for rapid recovery in five years—EBRD*. https://interfax.com/newsroom/top-stories/90538/
6. EU Parlament. (2022). *Corporate Sustainability Reporting Directive (CSRD) explained*. Https://Www.Carbontrust.Com/News-and-Insights/Insights/Corporate-Sustainability-Reporting-Directive-Csrd-Explained. https://www.carbontrust.com/news-and-insights/insights/corporate-sustainability-reporting-directive-csrd-explained
7. ISO14001. (2023b, 20 January). *ISO - ISO 14001 and related standards—Environmental management*. ISO. https://www.iso.org/iso-14001-environmental-management.html
8. PIMEE. (2023c). *G.E. Pukhov Institute for Modelling in Energy Engineering – National Academy of Sciences of Ukraine*. https://ipme.kiev.ua/en/home-page/
9. Prazian, M. (2023). Resilience for Better Sustainability. ISO 28000: 2022 vs 2007. Comparative Analysis. *Ядерна та радіаційна безпека*, *1(97)*, 67–70. https://doi.org/10.32918/nrs.2023.1(97).08
10. Regulation (EU) 2019/2088. (2019). *Sustainable Finance Disclosures Regulation*. https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/sustainable-finance-disclosures-regulation_en
11. TCFD. (2017). *Task Force on Climate-Related Financial Disclosures | TCFD)*. Task Force on Climate-Related Financial Disclosures. https://www.fsb-tcfd.org/
12. WRI. (2023d). *Greenhouse Gas Protocol*. World Resources Institute. https://www.wri.org/initiatives/greenhouse-gas-protocol
13. WRI, U. (2023). *Ambitious corporate climate action—Science Based Targets*. https://sciencebasedtargets.org/

M.M. Chaikin

OPPORTUNITY TO INTRODUCE CYBER RESILIENCE OF UKRAINE'S CRITICAL INFRASTRUCTURE IN THE ENERGY SECTOR AS PART OF REFORMING THE LEGAL AND REGULATORY FRAMEWORK FOR CYBERSECURITY

The relevance of cybersecurity of energy sector facilities has been especially evident since the beginning of the open aggression of the Russian Federation against Ukraine starting from February 24, 2022.

From the beginning of the military aggression, the occupiers showed a special interest in the capture and destruction of energy facilities. On February 24, 2022 the Kakhovskaya hydroelectric power station was captured. On 25 February, Russian troops blew up a gas pipeline near Kharkiv, Ukraine's second-largest city. On 2 March, 2022, Russia claimed to have taken control of the area surrounding the 5.7GW nuclear power plant in Zaporizhzhia, Europe's largest. In addition, during the period of autumn 2022 - spring 2023, the occupiers repeatedly launched rocket-bomb strikes specifically at energy facilities. At the same time, according to the analysis of the specialists of the ESET corporation, which works in close contact with the State Service for Special Communications and Information Protection of Ukraine, energy facilities were one of the priority targets of cyberattacks by the aggressor state [1].

Such activity of the enemy caused the accelerated modernization of requirements for the protection of critical infrastructure, including in cyberspace. At the beginning of last year, the state of regulatory regulation of cyber security issues was not fully determined. It is worth noting that the requirements for cyber security for critical infrastructure objects are described in the following legal documents:

- Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine [2];
- Law of Ukraine On information protection in information and communication systems [3];
- Resolution of the Cabinet of Ministers of Ukraine On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects [4];
- Law of Ukraine On Critical Infrastructure [5]

Law of Ukraine "About Critical Infrastructure" was entered into force on June 15, 2022 and finally defined a special body that will have to develop requirements for the protection of critical infrastructure and create a register of critical infrastructure objects – this body is State Service of Special Communications and Information Protection of Ukraine. Also, according to the text of the Law, a list of types of organizations is included, which, according to their type of activity, belong to critical infrastructure. Energy is included in this list. In addition, an important innovation of this law is the introduction of a risk-based approach and the requirement for insurance of security risks.

In 2021, the Administration of the State Service for Special Communications and Information Protection of Ukraine published Order No. 601 dated October 6, 2021, containing "Methodical recommendations on increasing the level of cyber protection of critical information infrastructure"[6]. Changes to this order, which were approved by the orders of the State Special Communications Administration dated 12.10.2021 No. 616 and dated 10.07, were published later. 2022 No. 343. These recommendations are developed taking into account the Framework for Improving Critical Infrastructure Cybersecurity issued in 2014 and updated in 2018 by the National Institute of Standards and Technology of the United States of America (NIST Cybersecurity Framework - NIST CSF) [7].

As a next step, on March 24, 2023, the Cabinet of Ministers of Ukraine adopted the Resolution on "Some issues of conducting an independent audit of information security at critical infrastructure facilities", which introduced a mandatory cyber security audit of critical infrastructure facilities every 2 or 3 years (depending on the category criticality)[8].

Since the State Service for Special Communications and Information Protection of Ukraine is responsible for the cyber protection of critical infrastructure objects, it can be stated that at the moment there are 3 different ways to confirm compliance with cyber security requirements, according to the 601st Order:

- Construction of a comprehensive information protection system with confirmed compliance (KSZI);
- Building an information security management system (ISMS);
- Audit for compliance with NIST CSF requirements and re-audit following implementation of recommendations.

In addition, it should be noted that some Ukrainian energy companies fall under the scope of regulation of the European Union in matters of cyber security. For example, the Ukrenergo company, as an operator of the dispatching and trunk transmission system, is part of the European network of electricity transmission system operators, which unites 43 operators in 39 countries of the European continent - ENTSO-E (European Network of Transmission System Operators for Electricity), which has and develops its cybersecurity requirements - Network code on energy cybersecurity.

The recast of the Electricity Regulation (Regulation (EU) 2019/943)[9] gives the Commission a mandate to develop a network code for cybersecurity. The Smart Grids Task Force has been doing preparatory work since 2017, and released its second interim report in July 2018. The report recommends setting up an early warning system for the energy sector in Europe, cross-border and cross-organisation risk management, minimum security requirements for critical infrastructure components, a minimum protection level for energy system operators, a European energy cybersecurity maturity framework and supply chain risk management.

In January 2022, the European Network of Transmission System Operators for Electricity (ENTSO-E) announced the details of its new cybersecurity code.

The Network Code on Cybersecurity(NCCS) is the first network code that will be developed according to the new rules established by the European Union on the internal market for electricity and is expected to enter into force by January 2024. The network code aims to set a European standard for the cybersecurity of cross-border electricity flows. It focuses on improving cybersecurity resilience through the enhancement of threat decision and incident reporting and proposes various measures to improve cybersecurity resilience that are essential to preserving the continuity of the services. On January 14, 2022, the preparation of the draft document was completed. [10]

At the same time, the State Service for Special Communications and Information Protection of Ukraine and the Cabinet of Ministers of Ukraine, with the active help of international partners, are working on updating Resolution No. 518 of the Cabinet of Ministers of Ukraine dated June 19, 2019 "On the approval of General requirements for cyber protection of critical infrastructure objects", which will lead to the acquisition of NIST CSF status is necessarily the standard for critical infrastructure facilities, instead of a recommendation status. This is a very important and timely step, as it will allow to synchronize the issue of cyber protection of critical infrastructure with the United States and implement a standard that was created specifically for critical infrastructure, as well as remove the variability of the choice of the approach by which to build cyber security at the objects of critical infrastructure.

Thus, it can be stated that at the moment in the Ukrainian regulatory and legal field there is an approach based on building cybersecurity, but not cyberresilience.

Cybersecurity and cyberresilience are related concepts but have distinct meanings in the context of digital security. While legislation varies between Europe and the USA, the following explanations provide general definitions and highlight the importance of prioritizing cybersecurity before focusing on cyber resilience in the energy sector:

- Cybersecurity: Cybersecurity refers to the measures and practices employed to protect digital systems, networks, and data from unauthorized access, damage, disruption, or theft. It involves the implementation of safeguards, technologies, and processes to prevent, detect, respond to, and recover from cyber threats. Cybersecurity focuses on safeguarding the confidentiality, integrity, and availability of information and systems.
  - Legislation in Europe: In Europe, the General Data Protection Regulation (GDPR) includes provisions related to cybersecurity, as it aims to protect personal data from unauthorized access or breach. Additionally, the EU Directive on Security of Network and Information Systems (NIS Directive) emphasizes the need for robust cybersecurity practices in critical infrastructure sectors, including energy.
  - Legislation in the USA: The United States has several cybersecurity-related laws, including the Federal Information Security Modernization Act (FISMA), the Cybersecurity Information Sharing Act (CISA), and the NIST Cybersecurity Framework. These laws promote the implementation of

cybersecurity measures across government agencies and critical infrastructure sectors, including the energy sector.

- Cyber resilience: Cyber resilience encompasses the ability of digital systems, networks, and infrastructure to withstand, adapt to, and recover from cyber threats, incidents, or disruptions. It involves a proactive and holistic approach that combines cybersecurity measures, incident response capabilities, and business continuity plans to ensure the continuity of critical operations and services.

  - Legislation in Europe: In Europe, the term "cyber resilience" is often used instead of "cyber stability." The NIS Directive addresses the need for enhancing the resilience of critical infrastructure, including the energy sector. It sets security and incident reporting requirements to improve the sector's preparedness for cyber incidents.
  - Legislation in the USA: In the USA, the concept of cyber resilience is typically incorporated within the broader framework of cybersecurity. The NIST Cybersecurity Framework, for instance, emphasizes the importance of resilience and the ability to recover from cyber incidents, ensuring the stability and continuity of systems and services.

Importance of prioritizing cybersecurity before cyber resilience:

1. Risk mitigation: Establishing a robust cybersecurity system is essential for identifying and mitigating vulnerabilities and threats. By prioritizing cybersecurity measures, organizations can reduce the likelihood and impact of cyber incidents. Mitigating risks and vulnerabilities lays the foundation for building cyber resilience.
2. Incident response readiness: Cybersecurity practices include incident response capabilities, enabling organizations to detect, respond, and recover from cyber incidents effectively. By establishing incident response protocols and processes, organizations are better prepared to manage and mitigate the impact of incidents. This readiness forms a crucial component of cyber resilience.
3. Regulatory compliance: Many regulatory frameworks, such as the NIS Directive in Europe or sector-specific requirements in the USA, emphasize the importance of cybersecurity for critical infrastructure sectors. Prioritizing cybersecurity ensures compliance with legal obligations and provides a strong foundation for achieving cyber resilience, which is necessary for maintaining the stability and continuity of critical energy infrastructure.
4. Business continuity: Cybersecurity measures directly contribute to the continuity of critical operations and services. By protecting systems and data, organizations can minimize disruptions and maintain the availability and reliability of energy services. A robust cybersecurity system serves as a prerequisite for establishing a resilient energy infrastructure.

While both cybersecurity and cyberresilience are crucial, prioritizing cybersecurity measures first allows organizations to address immediate risks, establish incident response capabilities, ensure regulatory compliance, and create a strong foundation for achieving cyber resilience in the energy sector.

When creating requirements based on the NIST Cybersecurity Framework for the cyber resilience of critical infrastructure in the energy sector in Ukraine, the following five problems can arise:

1. Limited awareness and understanding: One challenge may be the limited awareness and understanding of the NIST Cybersecurity Framework within the Ukrainian energy sector. The framework might not be widely known or comprehended by the stakeholders involved, which can hinder its effective implementation.

2. Resource constraints: Implementing the NIST Cybersecurity Framework requires dedicated resources, including skilled personnel, tools, and technologies. Ukraine's energy sector might face resource constraints, such as budget limitations or a shortage of qualified cybersecurity professionals, which can impede the successful implementation of the framework.

3. Regulatory misalignment: Ukraine may have its own existing cybersecurity regulations and standards that may not align perfectly with the NIST framework. Harmonizing these different requirements can be a complex task, leading to potential conflicts or redundancies that need to be resolved.

4. Legacy infrastructure: The energy sector often relies on legacy systems and infrastructure, which may have limited cybersecurity capabilities or be incompatible with the requirements set by the NIST framework. Upgrading or retrofitting these systems to meet the framework's standards can be costly and challenging, potentially causing delays and disruptions.

5. Information sharing and collaboration: The NIST Cybersecurity Framework emphasizes the importance of information sharing and collaboration among stakeholders to effectively manage cybersecurity risks. However, in Ukraine, there might be limited mechanisms or established platforms for such sharing and collaboration among energy sector entities. Building trust, establishing communication channels, and fostering cooperation can present significant challenges.

Addressing these problems requires a concerted effort from various stakeholders, including government agencies, energy sector organizations, and cybersecurity experts. It involves raising awareness, allocating resources, adapting regulations, modernizing infrastructure, and promoting collaboration to ensure the successful implementation of the NIST Cybersecurity Framework for the cyberresilience of critical infrastructure in the energy sector in Ukraine.

1 A year of devastating cyber attacks in Ukraine: how threats attacked users and organizations, URL: https://www.eset.com/ua/about/newsroom/press-releases/malware/god-razrushitelnykh-kiberatak-v-ukraine-kak-ugrozy-atakovali-polzovateley-i-organizatsii/

2 Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine, URL: https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text Application date: 15.05.2022.

3 Law of Ukraine On information protection in information and communication systems, URL: https://zakon.rada.gov.ua/laws/show/80/94-вр?lang=en#Text (link is external) Application date: 15.05.2022.

4 Resolution of the Cabinet of Ministers of Ukraine On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects, URL: https://zakon.rada.gov.ua/laws/show/518-2019-п?lang=en#Text Application date: 15.05.2022.
5 Law of Ukraine On Critical Infrastructure, URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
6 Order No. 601 dated October 6, 2021 of Administration of the State Service for Special Communications and Information Protection of Ukraine "Methodical recommendations on increasing the level of cyber protection of critical information infrastructure", URL: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.
7 NIST Cybersecurity Framework, URL: https://www.nist.gov/cyberframework.
8 Resolution of the Cabinet of Ministers of Ukraine "Some issues of conducting an independent audit of information security at critical infrastructure facilities", URL: https://www.kmu.gov.ua/npas/deiaki-pytannia-provedennia-nezalezhnoho-audytu-informatsi inoi-bezpeky-na-s257-240323.
9 Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast), URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0943&from=EN.
10 Network Code on Cybersecurity Drafting Status, URL: https://www.entsoe.eu/network_codes/nccs/.

A.A. Vladimirsky, I.A. Vladimirsky, I.P. Krivoruchko, G.V. Anfimova

TASK OF MONITORING UNDERGROUND PIPELINES OF NPP PROCESS WATER SYSTEMS AS A MEANS OF ENSURING RESILIENCE OF NUCLEAR POWER FACILITIES

Within the framework of the research work on the priority area "Technologies of Heat, Electricity and Nuclear Energy for Ensuring Energy Security of Ukraine", it is planned to develop and test a methodology for periodic monitoring of underground pipelines of service water systems of responsible NPP consumers based on the use of an active acoustic correlation parametric method for pipeline diagnostics being developed at the Institute. The purpose of the proposed research is to ensure the resilience of nuclear power facilities in Ukraine. A new correlation parametric method of acoustic signal research will be used to develop a diagnostic instrumentation complex for periodic monitoring of underground pipelines of process water systems of responsible consumers of nuclear power plants by detecting damage at the early stages of their occurrence, and it is planned to create a new competitive technology for detecting damage to underground pipelines at the early stages of their development.

The social and economic significance of the development of a diagnostic instrumentation complex for periodic monitoring of underground pipelines of process water systems of responsible NPP consumers by detecting damage at early stages of their occurrence is as follows. Ukrainian NPP sites have a developed network of underground pipelines of normal operation systems important for safety, failure of which may lead to failure of NPP safety systems and have a negative impact on the performance of safety functions. An example of such a system is the process water system of responsible consumers of NPPs (hereinafter referred to as PWSN), which provides a normal safety system of safety class 3 (classification designation - 3NZ according to NP 306.2.141-2008 "General Safety Provisions for Nuclear Power Plants"), group C (NP 306. 2.227-202 Safety Requirements for the Installation and Operation of Equipment and Pipelines at Nuclear Power Plants), the first category of seismic resistance (NP 306.2.208-2016 Requirements for Seismic Design and Seismic Safety Assessment of Nuclear Power Units). The SSCS is designed to remove heat from the reactor core through the emergency coolant exchanger, remove heat from the spent fuel pool, safety system mechanisms, etc. The system pipelines are laid underground at a depth of 2-6 meters. Given the safety impact, the SFSF is part of the NPP Ageing Management Program. Based on the results of the ENSREG peer review in 2017 on the topic of "ageing management", it was decided to develop a special program for the ageing management of the underground SFSF pipelines. Important components of the ageing management task are improving the detection of defects at early stages of their occurrence and improving the visibility and clarity of the forms of presenting operational information on the condition of the facility. Due to the inaccessibility of the ISFSF pipelines for external and internal inspection, it is

necessary to use non-contact inspection methods. Monitoring and assessment of the technical condition of underground pipelines of technological systems important for safety is an urgent task in the process of operating NPPs. To solve this problem, methods tested in other industries, where oil pipelines, gas pipelines, pipelines of public utilities, etc. are in operation, can be applied. In this work, on the basis of the developed parametric correlation method for determining the coordinates of pipeline damage [1, 2] and the active correlation parametric diagnostic method, it is planned to create an instrumentation complex for diagnosing underground pipelines and to develop a methodology for its application in the search for damage to pipelines of process water systems of responsible consumers of nuclear power plants.

The general research plan is to conduct theoretical and experimental studies and, based on their results, develop a scientifically sound methodology, methods and means for assessing and ensuring the resilience of the electric power industry on the example of nuclear power facilities in Ukraine:

- Development of an active acoustic correlation parametric method for diagnostics of underground pipelines and its implementation by creating an instrumentation complex for diagnostics of underground pipelines of technical water systems of responsible consumers of nuclear power plants.

- Development and testing of a methodology for periodic monitoring of underground pipelines of technical water systems of responsible consumers of NPPs based on the use of an active acoustic correlation parametric method of pipeline diagnostics. It is also envisaged that the hardware and software parts of the instrumentation complex may be corrected in the process of developing the methodology.

1. Patent No. 149956. Parametric correlation method for determining the coordinates of pipeline damage . Publication of information on December 15, 2021, Bull. No. 50 . Vladimirskyi O.A., Vladimirskyi I.A.
2. A. Vladimirsky, I. Vladimirsky, O. Dybach. Parametric Analysis of Correlation Functions for Acoustic Monitoring and Assessment of Underground Piping at NPPs. *Nuclear and Radiation Safety* . 2022. No. 3(95). pp. 64-70.

O.O Ogir, O.V. Tsurkan

EMPOWERING EPES AGAINST CYBER, PRIVACY, AND DATA ATTACKS WITH A NEW-GENERATION ELECTRON PLATFORM

ELECTRON is EU H2020 SU-DS04-2018-2020 funded research project that aims at delivering a new-generation EPES platform, capable of empowering the resilience of energy systems against cyber, privacy, and data attacks.

In the era of hyper-connected digital economies, the smart technologies play a vital role in the operation of the Electrical Power and Energy Systems (EPES), transforming it into a new, decentralized model with multiple benefits, such as distributed generation, pervasive control, remote monitoring and self-healing. Emerging Electrical Power and Energy Systems (EPES) act as a reliable backbone and springboard for tackling many of the current economic, environmental and societal challenges. They are mainly composed of distributed energy resources, transmission and distribution infrastructures, and increasingly advanced end-users and prosumers, which play an active and increasing role in the management of the electrical (smart-)grids.

EPES is going to constitute the greatest paradigm of the Internet of Things (IoT) [1]. However, although this new reality introduces significant advantages, it also raises crucial security and privacy risks due to the heterogeneous characteristics of the involved legacy and smart energy systems. In particular, EPES includes legacy systems, such as Supervisory Control and Data Acquisition System/Industrial Control Systems (SCADA/ICS) that rely on protocols designed without having security in mind. Therefore, EPES is exposed against a plethora of cyberattacks and malware, including Denial of Service (DoS), data privacy breaches, and ransomware. A new approach is needed for shielding EPES against cyberattacks, privacy violation, and data leaking.

The Ukrainian power grid constitutes the energy gates of Europe to the East. As a result, Ukraine becomes very often a challenging target for launching cyberattacks, data attacks, and personal attacks. On December 23, 2015, a ‘temporary malfunction’ of the power supply in three provinces in Ukraine resulted in power outages that lasted up to six hours and affected 223,000 customers. In addition, this incident was not the only one. Following the event, an investigation, identified evidence that several regional Ukraine power control systems, had been compromised by cyberattacks. Nevertheless, this incident was one of the most known cybersecurity episodes, having a high-impact, across Europe and globally. In addition, this was the first publicly documented successful cyberattack on a national grid, which was followed by many questions and investigations. It is obvious that such an incident – having so high impact – could be connected to attacks on the media and to targeted cyber-espionage attacks against Ukrainian governmental agencies. This is for sure a threat to the Ukrainian governmental

assets, while it could be potentially a threat to the freedom and security of Europe and its citizens.

Some of the key features that a new-generation EPES platform might include to enhance energy infrastructure resilience could include:

- Advanced encryption technologies to secure sensitive data and prevent unauthorized access to critical systems and infrastructure.
- Real-time threat detection and monitoring systems that can identify potential attacks before they occur or mitigate the impact of an ongoing attack.
- Secure communication protocols to protect against interception, data tampering, and other privacy and data attacks.
- Advanced access control systems to ensure that only authorized personnel have access to sensitive systems and data.
- Rapid incident response capabilities to quickly identify and contain cyber-attacks, minimize damage and restore system operations.

A new-generation EPES platform that incorporates advanced technologies and security measures can help to strengthen the resilience of energy systems against cyber, privacy, and data attacks, and provide greater confidence in the security and reliability of energy infrastructure. The Ukraine power grid hack incident in 2015 was a significant event that highlighted the vulnerability of critical infrastructure systems to cyber-attacks. In response to this incident, many organizations and cybersecurity experts have developed use cases and scenarios that explore the potential consequences of a similar attack and how to prevent it.

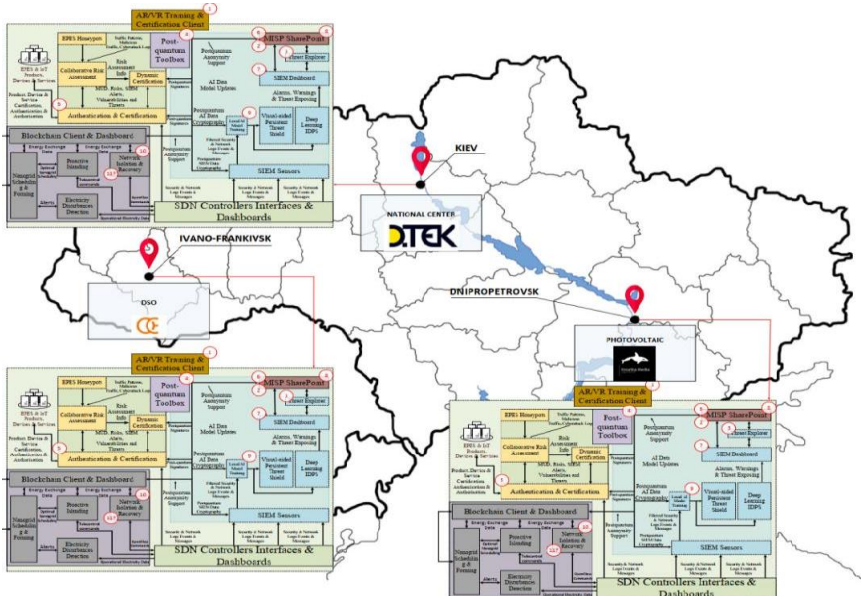


Figure 1 – Use Case 1 Architecture

One of ELECTRON Use Case1 inspired by the Ukraine power grid hack incident might involve a scenario where a group of hackers gain access to a utility company's network and deploy malware that allows them to take control of critical systems, including power generation and distribution. The attackers then proceed to disrupt the energy supply, causing a widespread power outage that affects thousands of homes and businesses.

To prevent this scenario from occurring, the Use Case might explore a range of cybersecurity measures and response actions, such as:

- Implementing multi-factor authentication and access controls to prevent unauthorized access to critical systems.
- Deploying network monitoring tools to detect and respond to unusual activity on the network.
- Regularly backing up critical data to prevent loss and ensure quick recovery in case of an attack.
- Conducting regular cybersecurity training and awareness programs for employees to recognize and respond to cyber threats.
- Developing and implementing a comprehensive incident response plan that includes strategies for identifying and mitigating cyber-attacks, as well as procedures for communicating with customers and the public in the event of a disruption.
- Regularly conducting penetration testing and vulnerability assessments to identify and address potential weaknesses in the system.

ELECTRON Use Case1 inspired by the Ukraine power grid hack incident can provide valuable insights into the potential consequences of a cyber-attack on critical infrastructure systems and help organizations to develop effective strategies for prevention and response.

1. Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware
2. Ukrainian Power Grid Attack Makes History https://www.globalsign.com/en/blog/cyber-autopsy-series-ukranian-power-grid-attack-makes-history

A.A. Vladimirsky, V.O. Artemchuk, V.A. Dyukov, I.A. Vladimirsky

TASK OF CREATING DIAGNOSTIC TOOLS FOR NUCLEAR POWER PLANT STEAM GENERATORS AS A MEANS OF ENSURING RESILIENCE OF NUCLEAR POWER FACILITIES

Within the framework of the research work on the priority area "Technologies of Heat, Electricity and Nuclear Energy for Ensuring Energy Security of Ukraine", it is planned to develop and master the production of technical means for diagnosing damage to VVER-1000 nuclear power plant steam generator tubes in Ukraine. The purpose of the proposed research is to ensure the resilience of nuclear power facilities in Ukraine. The social and economic significance of developing and mastering the production in Ukraine of technical means for diagnosing damage to the VVER-1000 nuclear power plant steam generator tubes is as follows. A steam generator is one of the main elements of a nuclear power plant reactor. A modern domestic VVER-1000 reactor has four circulation loops of the first circuit coolant. In each coolant circulation loop, a PGV-1000M steam generator is installed, the main function of which is to generate dry saturated steam due to heat transferred to the steam generator from the nuclear reactor core by the first circuit coolant. The steam generator for NPPs with VVER reactors is a recuperative heat exchanger. The primary coolant with a temperature of more than 300°C flows from the nuclear reactor through a hot pipeline to the steam generator's hot header, from which the coolant enters a tube bundle of heat exchange tubes consisting of 11,000 U-shaped coils, and then to the cold header, from which the coolant is pumped through the pipeline by the main circulation pump to the nuclear reactor. circulation pump into the nuclear reactor. The cold water of the second circuit, which enters the internal volume of the steam generator, is heated to steam. This process is accompanied by the accumulation of deposits of corrosion products coming with the coolant on the heat exchange surface and the concentration of corrosive impurities in them. As the thickness of the deposits increases, the concentration of chlorides in them increases, reaching critical values at the surface of the tubes, at which the protective oxide film on the steel, which is the structural material of the heat exchange tubes, is destroyed. Localized metal surface defects appear and develop. Corrosion cracking of the material leads to failure of the heat exchange tubes. This development poses a very serious safety hazard. Taking into account the above potential threats to NPP operation safety, the development and implementation of methods and technical means for effective diagnostics of the technical condition of tube bundles of steam generator heat exchange tubes is an extremely urgent task. The diagnostic results should be used to assess their technical condition, determine their residual service life and develop correct and reasonable management decisions on their continued operation.

Analyzing the world experience in the context of technical means for diagnosing damage to VVER-1000 steam generator tubes, it should be noted that deficiencies in the structural materials of heat exchange tubes of steam generators

of domestic VVER-1000 reactors were revealed during operation. A huge amount of research and technical measures, including those related to ensuring the required quality of the water-chemical regime of the second circuit and improving the coolant treatment systems, did not lead to a radical solution to the problem. In the course of operation of domestic steam generators, they are subject to degradation, which is accompanied by salt deposits, corrosion cracking, and leaks. This development poses a very serious safety hazard. Currently, heat exchange tubes are inspected using the eddy current method. Eddy current testing is considered fast, simple and accurate. However, with regard to heat exchange tubes of steam generators of domestic VVER-1000 reactors, there are serious problems associated with transportation of probes along thin heat exchange tubes (diameter about 12 mm) over a long distance (more than 10 m). The service life of imported sensors, despite their high cost, is low. Therefore, the task of developing and mastering the production of domestic probes with an extended service life, improved characteristics and affordable price is extremely urgent. By improving the quality of diagnostics of steam generator tube bundles, the probability of leaks at the interval between maintenance intervals should be reduced and the need for an emergency shutdown of a nuclear facility should be excluded. At the same time, the quality of diagnostics of steam generator tube bundles should be improved due to: 1) development and mastering of the production of appropriate technical diagnostic tools in Ukraine; 2) development and implementation of appropriate scientifically based diagnostic methods.

O.S. Potenko

ANALYSIS OF ACTUAL INFORMATION SECURITY VULNERABILITY DATABASES

Every year, the number of new security vulnerabilities, both in software and in hardware, is constantly increasing. To counteract this, constant monitoring and tracking of new vulnerabilities, timely updating and use of up-to-date protection systems are required. The problem of vulnerabilities and their detection has been studied for a long time, and various attempts have been made to classify vulnerabilities according to different criteria. This has made it possible to create databases of vulnerabilities that allow them to be tracked, analyzed and quickly countered. Analysis of actual information security the most popular databases and catalogs of vulnerabilities is actuals task of this article.

MITRE CVE

The CVE (Common Vulnerabilities and Exposures) standard was launched in 1999 by the American non-profit research corporation MITER to identify and classify vulnerabilities in software and hardware firmware. CVE provides a free database for organizations to improve their cybersecurity. MITER is a not commercial organization that operates federally funded research and development centers in the United States. CVE standard is currently the main standard in the field of uniform naming and registration of identified software vulnerabilities. CVE identifiers allow security professionals to access information about specific cyber threats from multiple information sources using a common identifier. As of 2013, the database has 200,000 CVE records [1].

CVE identifiers have the format CVE-YYYY-NNNN, with the first four digits showing the year the vulnerability was registered and the following digits the unique vulnerability number within that year.

For each of the identified vulnerabilities, the record in the database contains a brief description of the type and causes of the vulnerability, vulnerable software versions, a criticality assessment of the vulnerability according to the CVSS (Common Vulnerability Scoring System) standard, and links to external sources with information about the vulnerability.

NVD

NVD (National Vulnerability Database) is a US government repository of standardized vulnerability data presented using the SCAP protocol. This data enables the automation of vulnerability management, security measurement, and security compliance [2].

NVD includes a database of security checklists, security-related software flaws, misconfigurations, product names, and exposure metrics.

NVD performs analysis of CVEs that have been published in the CVE Dictionary. NVD staff are tasked with analyzing CVEs by aggregating data points from the description, provided links, and any additional data that can be found in the public domain at this time. The result of this analysis are association impact

metrics (Common Vulnerability Scoring System - CVSS), vulnerability types (Common Weakness Enumeration - CWE) and usage statements (Common Platform Enumeration - CPE), as well as other relevant metadata.

VulnDB

VulnDB is the most comprehensive and timely vulnerability analytics offering actionable information on the latest security vulnerabilities through an easy-to-use SaaS portal or RESTful API that provides easy integration with GRC tools and ticketing systems.

VulnDB allows organizations to search and receive notifications about the latest vulnerabilities in both user software and third-party libraries or dependencies. VulnDB is a paid database. By 2023, the database includes more than 300,000 vulnerabilities, 100,000 of which are absent in the CVE system [3].

VND CERT/CC

The VND (Vulnerability Notes Database) US-CERT Vulnerability Notes database is owned by CERT, which is part of the Software Engineering Institute, a federally funded research and development center administered by Carnegie Mellon University [4].

Each entry in the VND database aggregates information about a set of similar vulnerabilities for any particular software, referring to a set of corresponding CVE identifiers. This aggregation is a characteristic difference of the VND database from the CVE List and NVD databases, allowing to check many vulnerabilities of the same type in a specific vulnerable software or its components.

Also, entries in the VND database contain ways to eliminate vulnerabilities and prevent their exploitation by an attacker.

The situation with the presence or successful closure of identified vulnerabilities by various vendors is also monitored.

Conclusion: Vulnerability databases are a valuable and relevant resource for securing information systems. Vulnerability databases contain information about various vulnerabilities in software, operating systems, and other information system components. They allow you to identify vulnerabilities that can be exploited by attackers. Vulnerability databases allow you to evaluate vulnerabilities according to their potential consequences. All this helps organizations and security teams analyze vulnerabilities and take actions to prevent them. Regular database updates allow system administrators to quickly respond to vulnerabilities and apply appropriate security measures, such as installing patches or updates. Also, Vulnerability Databases serve as a research tool for security professionals and scientists to analyze and study vulnerabilities. You can find the latest versions of the threat databases at the references below.

1 CVE main opage https://cve.mitre.org/
2 VND main opage https://nvd.nist.gov/general
3 About VulnDB https://vulndb.cyberriskanalytics.com/
4 SEI CERT Coordination Center. https://www.kb.cert.org/vuls/

С.Є. Саух

КОНЦЕПЦІЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ЕНЕРГЕТИКИ В УМОВАХ ТЕРОРИСТИЧНИХ ТА МІЛІТАРНИХ ЗАГРОЗ

На сьогодні стійкість енергетичного сектора забезпечується організаційно-технологічними та технічними рішеннями проблем стійкості, робастності, довговічності та резильєнтності електроенергетичної системи (ЕЕС).

Стійкість – це здатність ЕЕС повертатися до усталеного режиму роботи після збурень без переходу до асинхронного режиму [1,2]. Стійкість ЕЕС визначається як статична та динамічна. Статична стійкість – це здатність ЕЕС повертатися до усталеного режиму після незначних збурень, за яких зміни системних параметрів (кут, напруга, потужність) малі проти їх середніх значень; динамічна стійкість – це здатність ЕЕС повертатися до усталеного режиму після значних збурень.

Робастність – це здатність ЕЕС зберігати свою функціональність при змінах параметрів системи та невизначеності зовнішніх впливів, зокрема, здійснювати демпфірування коливань потужності шляхом зменшення впливу електромеханічних перехідних процесів, пов'язаних з рухом роторів електричних машин, спричинених порушенням балансу між механічним моментом на валу машини та електромеханічним моментом [2,3]. Робастність досягається створенням адаптивної інфраструктури та системними інноваціями.

Резильєнтність – це здатність енергетичного сектору адаптуватися до шокових загроз та стресових навантажень, а також протистояти, реагувати та швидко відновлюватися після дії таких збурень [4].

Довговічність – це здатність ЕЕС підтримувати виконання поточних і планових ремонтних робіт та робіт з технологічного оновлення енергетичного устаткування, стимулювати розвиток нових джерел та носіїв енергії, здійснювати технологічні переходи, поглиблювати взаємодію між виробниками енергетичних продуктів, забезпечувати втілення ринкових механізмів управління енергетичним сектором.

Як сектор економічної діяльності, енергетичний сектор у складі ЕЕС і системи організаційно-технологічного управління та реагування є стійким лише в умовах нецілеспрямованих дій шокових загроз та стресових навантажень [5].

Цілеспрямовані терористичні та мілітарні загрози енергетичному сектору спостерігаються та реалізуються в багатьох країнах сучасного світу [6]. Винятковий характер дії таких загроз обумовлений метою їх планування та реалізації – руйнування цілісності ЕЕС та утворення енергетичних островів з суттєво обмеженими або взагалі відсутніми можливостями виробляти, передавати та постачати електроенергію її споживачам. За таких обставин сукупність технічних рішень лише проблем стійкості, робастності,

довговічності та резильєнтності ЕЕС не є достатньою для забезпечення стійкості енергетичного сектора.

Стійкість енергетичного сектора в умовах дії терористичних та мілітарних загроз необхідно забезпечувати організаційно-технологічними та технічними рішеннями ще однієї проблеми – проблеми структурної мінливості ЕЕС.

Структурна мінливість – це здатність ЕЕС формувати таку кількість підсистем і електричних з'єднань між ними, яка надає можливість системному оператору управляти структурою ЕЕС і, у такий спосіб, забезпечувати жорстку стійкість енергетичного сектора в умовах цілеспрямованих руйнівних дій.

Декарбонізація є актуальною стратегією розвитку ЕЕС багатьох країн світу. В умовах руйнівних мілітарних дій така стратегія розвитку ЕЕС України не є самодостатньою. Потребує обов'язкового втілення ще одна енергетична стратегія – побудова структурно мінливої ЕЕС, тобто такої, цілеспрямоване ураження якої не призводить до тривалого знеструмлення великих груп споживачів.

Концепція забезпечення структурної мінливості ЕЕС, як стратегія випередження викликів і загроз, збереження і розвитку електроенергетичного сектора України, представлена нижче.

Побудову структурно мінливої ЕЕС необхідно починати з регіонального рівня. В кожній регіональній ЕЕС мають бути встановлені генеруючі потужності та системи зберігання енергії, які сумарною потужністю спроможні забезпечити виробництво електроенергії в обсягах, достатніх для споживання населенням, житлово-комунальними господарствами, транспортом та сільським господарством цього регіону. Забезпечення електроенергією власного регіонального виробництва зазначених категорій споживачів дозволяє максимально убезпечити життєдіяльність кожного регіону від впливу руйнівних дій, спрямованих на ОЕС України або на інші регіональні ЕЕС.

Визначення меж ЕЕС регіону встановлюється відповідно до наступних двох чинників. Відповідно до вимог стійкості енергетики структурна мінливість ЕЕС країни може забезпечувати більшу її стійкість у разі поділу на регіональні ЕЕС якомога меншого розміру. Разом з тим, кожна регіональна ЕЕС повинна задовольняти попит на електроенергію споживачів, які спроможні відшкодовувати експлуатаційні та капітальні витрати регіональних енергетичних компаній. Таким чином межі ЕЕС регіонів встановлюються на основі компромісу між вимогами щодо стійкості енергетики та рівнів капіталізації регіонів.

Кожна регіональна ЕЕС може працювати ізольовано в режимі енергетичного острова або у складі ЕЕС країни.

ОЕС України підтримує регіональні ЕЕС узгодженими обсягами маневрових і резервних потужностей та забезпечує постачання електроенергії підприємствам промислової, будівельної, транспортної та іншим видам економічної діяльності, які мають національне значення і не

приєднуються до регіональних ЕЕС. У випадках руйнування окремих регіональних ЕЕС національна ОЕС України, а також сусідні регіональні ЕЕС разом забезпечують нагальні потреби потерпілих регіонів в електроенергії в обсягах, достатніх для споживання населенням, житлово-комунальними господарствами, транспортом та сільським господарством.

В структурно мінливій ЕЕС країни механізми управління господарською діяльністю енергетичних компаній мають бути єдиними для всіх учасників ринку як на національному, так і на регіональному рівнях. Для цього можуть застосовуватись механізми декомпозиції торгівельних площадок [7].

Розроблення математичних моделей регіональних ЕЕС та моделі структурно мінливої ЕЕС країни є необхідною умовою планування оптимального розвитку енергетики. На сьогодні завершено розроблення математичної моделі регіональних ЕЕС з великими частками виробництва електроенергії установками ВЕС, СЕС та АЕС на малих модульних реакторах, а також системами збереження енергії. Таким чином створено інструмент планування розвитку окремих регіональних ЕЕС [8].

1. Стійкість енергосистем. Керівні вказівки. – К.: ОЕП "ГРІФРЕ". – 2002. – 23 с.
2. Буткевич О.Ф., Кириленко О.В., Леньга О.В., Лук'яненко Л.М., Павловський В.В., Стелюк А.О., В.В.Чижевський. Забезпечення стійкості енергосистем та їх об'єднань. – К.: Ін-т електродинаміки НАН України. – 2018. – 320 с.
3. Кодекс системи передачі. Затверджено Постановою НКРЕКП № 309 від 14.03.2018. – 201 с.
4. Stout S., Lee N., Cox S., Elsworth J., Leisch J. Power sector resilience planning guidebook. – U.S. Department of Energy's NREL and USAID. – 2019. – 82 p. – URL https://www.nrel.gov/docs/fy19osti/73489.pdf.
5. Stirling A. From Sustainability, through Diversity to Transformation: towards more reflexive governance of technological vulnerability. *Vulnerability in Technological Cultures: new directions in research and governance.* MIT Press. 2014. Pp. 305 – 332.
6. Mitoulis S.-A., Argyroudis S., Panteli M., Fuggini C., Valkaniotis S., Hynes W., Linkov I. Conflict-resilience framework for critical infrastructure peacebuilding // Sustainable Cities and Society. – 2023. – vol. 91, 104405. URL https://doi.org/10.1016/j.scs.2023.104405.
7. Saukh S., Borysenko A. Modelling of market equilibrium on the basis of Smart Grid market system decomposition. Proc. 7th International Conference on *Energy Smart Systems*. Kyiv. 2020. Pp. 358-362. URL: https://doi.org/10.1109/ESS50319.2020.9160333.
8. Saukh S., Borysenko A. Mathematical Model of a Local Grid with Small Modular Reactor NPPs. *Nuclear & Radiation Safety*. 2022. No 1, Pp. 44 – 52. URL: https://doi.org/10.32918/nrs.2022.2(94).05.

О.М. Суходоля

СТІЙКІСТЬ ФУНКЦІОНУВАННЯ ІНФРАСТРУКТУРИ ТА ЗАБЕЗПЕЧЕННЯ ЖИТТЄДІЯЛЬНОСТІ ГРОМАД: ІМПЛЕМЕНТАЦІЯ ПОЛОЖЕНЬ ЗАКОНУ УКРАЇНИ «ПРО КРИТИЧНУ ІНФРАСТРУКТУРУ»

Закон України «Про критичну інфраструктуру» [1] визначає завдання, для місцевих органів влади, забезпечити розроблення та затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури (КІ), програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних порушенням функціонування КІ. Розроблення таких програм потребує чіткого визначення предмету програм, розроблення методичних засад їх розроблення та реалізації.

При цьому, законом уже визначено загальну рамку діяльності у цьому напрямі, зокрема дається визначення «стійкість критичної інфраструктури»[1] та наголошується на необхідності взаємодії залучених суб'єктів у різних режимах функціонування КІ (*штатний, готовність та запобігання, реагування та відновлення*).

Відповідно до цього Плани забезпечення стійкості КІ та стійкості територіальних громад до кризових ситуацій мають відображати заходи та взаємодію суб'єктів у всіх режимах функціонування КІ (*Таблиця 1*).

Таблиця 1 – Приклади заходів та процедур взаємодії суб'єктів

Режими	**Приклади заходів**
Готовність Preparedness	Захист КІ відповідно до визначеного рівня загроз/небезпек; Плани взаємодії залучених суб'єктів та плани реагування; Навчання персоналу; Обмін інформацією про кращі практики; Аналіз безпекової ситуації та оцінка ризиків;
Пом'якшення / запобігання Mitigation	Модернізація об'єктів КІ та оновлення обладнання відповідно до визначених ризиків; Резервування систем, накопичення запасів; Плани «заміщення» пошкодженого обладнання, втрачених ресурсів чи функцій іншими активами та суб'єктами; Накопичення запасів та резервів;
Реагування Response	Залучення «проектних» сил та ресурсів відповідно до визначених планів реагування на визначені типи загроз; Залучення «додаткових» місцевих сил та ресурсів; Аналіз ситуації та координація реагування;

[1] стійкість критичної інфраструктури - стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду

Відновлення Recovery	Заміна/ремонт КІ, будівель, обладнання; Рішення з тимчасового відновлення функцій/послуг; Рішення з відновлення повноцінного функціонування з врахуванням необхідності підвищення стійкості у майбутньому та нових технологічних можливостей;

Для розроблення планів стійкості функціонування КІ та життєдіяльності громади доцільно сформувати Планувальну групу, яка включатиме у себе представників усіх зацікавлених. Діяльність з розроблення планів стійкості має включати наступні етапи [2]:

усвідомлення соціально-економічних аспектів життєдіяльності громад та цілей розвитку інфраструктурних систем;[2]

усвідомлення взаємозалежностей функцій/послуг та/чи КІ;[3]

визначення актуальних загроз (і сценаріїв їх реалізації) та оцінка ризиків життєдіяльності громад; [4]

встановлення необхідних (бажаних) цільових параметрів надання функцій/послуг та/чи функціонування КІ (допустимий рівень, мінімально необхідний, час реагування тощо);[5]

визначення очікуваної ефективності реагування на визначені сценарії реалізації загроз інфраструктурним системам (об'єктам);

визначення «прогалин» спроможностей, як відхилення параметрів необхідного та очікуваного рівня функціонування КІ (*Таблиця 2*);

формування конкретного переліку заходів усунення «прогалин» залежно від інфраструктурної системи, технологічних та географічних особливостей.

---

[2] Усвідомлення соціально-економічних аспектів є вихідним кроком для визначення переліку життєво-важливих функцій/послуг, необхідних для забезпечення стійкості життєдіяльності громади.

[3] Існують різні типи взаємозалежностей інфраструктури, серед найбільш поширених виділяють: фізичні (наприклад, входи та виходи однієї інфраструктури використовується іншою; кібер (електронні, управлінські, інформаційні зв'язки); Географічні (розміщення на одній/суміжній території чи спільний маршрут ланцюжків постачання вхідних ресурсів/ виробленої продукції); Функціональні (наприклад, робота однієї інфраструктури допомагає роботі іншої хоча не відображається у фізичній залежності).

[4] При розробці сценаріїв реалізації загроз необхідно забезпечити врахування особливостей функціонування КІ (технологічні, природні, географічні тощо), щоб відображати події, які є найбільш вірогідними для визначеної громади та матимуть найбільший вплив на функціонування відповідної сфери.

[5] Встановлення бажаних цілей залежить від визначення двох основних факторів: (1) прийнятний рівень шкоди для певного рівня загрози; (2) час необхідний для відновлення нормального режиму функціонування КІ (рівня надання функцій/послуг.

Таблиця 2 - Визначення впливу загроз на функціонування КІ та ідентифікація прогалин у забезпеченні стійкості

Пріоритетні інфраструктурні системи (функції/послуги)	**Залучені суб'єкти реагування**	**Короткотермінові заходи**			**Середньострокові заходи**			**Довготривалі заходи**		
		0 - 1 година	до 24 годин	до 72 годин	до 7 днів	2-3 тижні	до 8 тижнів	3-6 місяців	6-12 місяців	Більше року
Інфраструктура забезпечення споживачів електроенергією (***Інфраструктура система 1,*** підстанція та розподільчі мережі)	Д, МВ, О, ЗС	**70%** ***50%***	**90%** ***70%***				***90%***			**Проект-ний рівень**
Система водопостачання (***Інфраструктура система 2***, насосна станція, трубопровідні мережі, водозабір***)***	МВ, О,	**30%**	**90%** ***30%***		***70%***		***90%***	**Проект-ний рівень**		
Інфраструктура постачання палива (***Інфраструктура система 3,*** нафтобаза та АЗС***)***	О, ЗС			**30%** ***30%***	**70%** ***70%***			**90%** ***90%***	**Проект-ний рівень**	
…..- …….										
Інфраструктурна система транспортування (***Інфраструктура система – N***, дороги, мости, гараж, автостанція***)***	Д, МВ, О, ЗС	**70%**	**90%** ***30%***		***70%***			***90%***		

Пояснення:

Залучені суб'єкти реагування: Д – Державні органи влади загальнодержавного рівня (Центральні органи виконавчої влади та їх регіональні підрозділи); МВ – Місцеві органи влади (Місцеві органи виконавчої влади, органи місцевого самоврядування); О – Оператори КІ, надання функцій/послуг; ЗС –залучені суб'єкти кризового реагування (інші суб'єкти);

Відсотки рівня зниження функціональності КІ: нормальний шрифт **(30%)** – необхідні (бажані) рівні функціональної спроможності КІ для підтримання життєдіяльності громади; підкреслений курсив (***70%***) – очікувані (фактичні) рівні функціональної спроможності КІ.

Різниця між необхідними та очікуваними рівнями визначають «прогалини» спроможностей реагування. Для усунення цього розробляються заходи забезпечення стійкості функціонування КФ та надання ЖВП.

Безумовно, проведений аналіз різних аспектів забезпечення стійкості функціонування КІ та життєдіяльності громад має бути формалізований у розпорядчих рішеннях та нормативних документах визначеного рівня.

Одним із основних таких документів є формалізований план стійкості. Для цілей формування єдності методологічних засад розроблення таких планів та координованості реалізації державної політики у сфері захисту КІ доцільно затвердити, рішенням Уповноваженого органу у сфері захисту КІ, типову структуру таких планів.

Примірний зміст та структура плану стійкості може бути наступним:

1. **Цілі розвитку громади** - визначення цілей розвитку громади, оцінка соціально-економічної ситуації, наявних активів на території громади;
2. **Пріоритети стійкості життєдіяльності громади** - визначення переліку життєво-важливих функцій та послуг, які потребують стійкого функціонування інфраструктурних систем;
3. **Профіль громади -** усвідомлення та оцінка життєдіяльності громади з точки зору вимог до функціонування КІ, з врахуванням соціальних, економічних, технологічних, природно-географічних, ресурсних особливостей;
4. **Суб'єкти забезпечення стійкості -** визначення суб'єктів кризового реагування;
5. **Аналіз ризиків** - оцінювання загроз та ризиків порушення функціонування КІ та життєдіяльності громад;
6. **Розвиток спроможності громади -** посилення спроможності громади до реагування у кризовій ситуації (процедури взаємодії між суб'єктами реагування; контактні особи та обмін інформацією; проведення навчань та тренінгів для суб'єктів реагування);
7. **Забезпечення стійкості - визначення заходів забезпечення стійкості** (запобігання впливу загроз (захист КІ); пом'якшення наслідків реалізації загрози (резервування, заміщення); відновлення (ремонт, будівництво нового, переміщення споживання);
8. **Пріоритети розвитку** - вивчення уроків та розроблення довгострокових планів розвитку інфраструктури громади.

1. Закон України «Про критичну інфраструктуру». https://zakon.rada.gov.ua/laws/show/1882-20#n80
2. NIST Community Resilience Planning Guide https://www.nist.gov/community-resilience/planning-guide

Б.Д. Халмурадов, В.П. Федина, О.О. Козлітін

ДОСВІД ПІДГОТОВК КАДРІВ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У багатьох країнах світу цей безпековий напрям визнано пріоритетним у політиці національної безпеки. Відтак у цих країнах активно розбудовуються національні системи із забезпечення захисту (безпеки) та стійкості критичної інфраструктури, ухвалюються законодавчі документи для регламентації діяльності учасників системи, готуються відповідні кадри, налагоджуються партнерські відносини з приватним сектором, здійснюються освітні заходи серед населення тощо.[1]

Підготовка кадрів у сфері забезпечення захисту об'єктів критичної інфраструктури є важливим процесом, що передбачає отримання майбутнім фахівцем необхідний набір спеціалізованих знань і навичок для реалізації стійкості та безпеки об'єктів критичної інфраструктури.

Національний авіаційний університет починаючи з 2017 року здійсню підготовку фахівців у сфері забезпечення захисту об'єктів критичної інфраструктури, реалізуючи це через освітньо-професійну програму «Захист об'єктів критичної інфраструктури» на базі спеціальності 263 «Цивільна безпека». Осівтньо-професійна програма реалізується на кафедрі «Цивільної та промислової безпеки».

Основні загрози для критичної інфраструктури це: загрози природного і техногенного характеру, загрози, що спричинені протиправними діями, та інші загрози.[2]

Зміст Стандарту вищої освіти спеціальності 263 «Цивільна безпека» (бакалавр) вміщує в себе фахові компетенції та програмні результати навчання які спрямовані на попередження та мінімізацію наслідків від впливу згаданих загроз на функціонування підприємств.

Основний фокус осівтньо-професійної програми «Захист об'єктів критичної інфраструктури» полягає в одержанні знань з сучасних методів забезпечення захисту та стійкості об'єктів критичної інфраструктури, техногенної безпеки, а також реагування на надзвичайні ситуації та ліквідацію їх наслідків.

Зокрема фахові компетенції такі як «Здатність до оцінювання ризиків виникнення та впливу надзвичайних ситуацій на об'єктах суб'єкта господарювання та ризиків у сфері безпеки праці», «Здатність до аналізу й оцінювання потенційної небезпеки об'єктів, технологічних процесів та виробничого усталювання для людини й навколишнього середовища», «Здатність обґрунтовувати необхідність та розробляти заходи, спрямовані на запобігання виникненню надзвичайних ситуацій, захист населення і територій від надзвичайних ситуацій» та інші викладаються з урахуванням особливостей об'єктів критичної інфраструктури, що дозволяє здобувачам вищої освіти набути відповідні фахові компетенції.

Програмні результати навчання такі як «Ідентифікувати небезпеки та можливі їх джерела, оцінювати ймовірність виникнення небезпечних подій та їх наслідки», «Аналізувати і обґрунтовувати інженерно-технічні та організаційні заходи щодо цивільного захисту, техногенної та промислової безпеки на об'єктах та територіях», «Пояснювати вимоги щодо убезпечення та захисту суб'єктів господарювання, положення та вимоги щодо безпечності, ідентифікації, паспортизації та ведення реєстрів об'єктів підвищеної небезпеки та потенційно небезпечних об'єктів», «Знати вимоги щодо безпечності об'єктів підвищеної небезпеки та потенційно небезпечних об'єктів; основні положення та вимоги щодо ідентифікації та паспортизації об'єктів підвищеної небезпеки та потенційно небезпечних об'єктів; основні положення та вимоги до порядку ведення Реєстрів потенційно небезпечних об'єктів та об'єктів підвищеної небезпеки; Реєстру критичної інфраструктури», формують у майбутнього фахівця необхідні знання та навички для подальшої роботи.

Усі згадані фахові компетенції та програмні результати навчання реалізуються в окремих дисциплінах.

Хочемо наголосити, що на кафедрі перекладена, адаптована та імпламентована навчальна дисципліна «Основи стійкості критичної інфраструктури». Цей курс пропонує для випускників: вступ до політики, стратегії та практичного застосування безпеки та стійкості критичної інфраструктури з точки зору всіх небезпек. Він описує стратегічний контекст, представлений середовищем ризику 21 століття, і обговорює виклики та можливості, пов’язані з наступним: державно-приватне партнерство, пов’язане з інфраструктурою; обмін інформацією; аналіз ризиків та встановлення пріоритетів; зниження ризику; вимірювання продуктивності; управління інцидентами; а також планування та інвестування в невизначене майбутнє.

Висновки. Для кращій підготовки кадрів у сфері забезпечення захисту об’єктів критичної інфраструктури, кафедра потребує розширення баз практики, сучасні симулятори кризових ситуацій, прикладних програм для моделювання стійкості та безпеки об’єктів критичної інфраструктури.

1. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К. : НІСД, 2019. – 224 с.
2. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р //База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/1009-2017-%D1%80

В.В. Басистий

ОГЛЯД ПРОГРАМ З ПІДГОТОВКИ ФАХІВЦІВ ІЗ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Поточна ситуація в Україні. Українські державні, приватні, науково-дослідні установи та науковці почали активно розробляти та впроваджувати навчальні програми з питань захисту критичної інфраструктури в українській освітній системі з 2015 року. З того часу були розроблені різноманітні курси, програми та модулі для студентів державних та приватних університетів, що базуються на підходах кібербезпеки або фізичної безпеки для захисту об'єктів критичної інфраструктури. Всі ці навчальні програми частково інтегровані в навчальні плани вищих навчальних закладів за такими спеціальностями, як 125 "*Кібербезпека*", 263 "*Цивільний захист*", 081 "*Право*", 256 "*Національна безпека*" та 143 "*Атомна енергетика*".

Програми підготовки фахівців з кібербезпеки вже реалізуються у 59 університетах України в рамках спеціальності № 125 "*Кібербезпека*". Ця спеціальність була утворена шляхом об'єднання трьох спеціальностей старого переліку - "*Безпека інформаційних і комунікаційних систем*", "*Управління інформаційною безпекою*" та "*Системи захисту інформації*". Стандарт вищої освіти для першого (бакалаврського) рівня був затверджений 4 жовтня 2018 року. Університети мали лише два роки на затвердження та впровадження нових програм. Стандарт вищої освіти другого (магістерського) рівня був затверджений Міністерством освіти і науки України 18 березня 2021 року. Стандарт для третього (докторського) рівня перебуває на стадії розробки.

Україна також досягла прогресу в додаванні нових 26 професій у сфері інформаційної безпеки та кібербезпеки до класифікатора професій.

Національне агентство кваліфікацій внесло до Реєстру кваліфікаційні відомості щодо професійних стандартів:

- «*Розробник систем захисту інформації*»;
- «*Адміністратор мереж і систем*»;
- «*Фахівець сфери захисту інформації*»;
- «*Аналітик з безпеки інформаційно-телекомунікаційних систем*»;
- «*Фахівець з питань безпеки (інформаційно-комунікаційні технології)*»;
- «*Інструктор-методист з інформаційної безпеки та кібербезпеки*».

Станом на 2022 рік їх у класифікаторі було лише дві: "*Професіонал з інформаційної безпеки*" та "*Фахівець з інформаційної безпеки*". Внесення цих профстандартів до Реєстру кваліфікацій означає, що відтепер заклади вищої освіти можуть використовувати ці стандарти для вдосконалення освітніх програм та запровадження спеціалізації, а самі фахівці та роботодавці – для оцінки відповідності рівня знань, умінь та навичок актуальним потребам галузі.

У порівнянні з навчальними планами та програмами з кібербезпеки, навчальні програми із захисту критичної інфраструктруи (ЗКІ) перебувають все ще на початковій стадії розвитку у формальній системі вищої освіти України. Наразі курс "*Об'єкти захисту критичної інфраструктури*" впроваджується в рамках бакалаврської програми спеціальності №263 "*Цивільний захист*", а в навчальні плани приватних навчальних закладів також включено курс "*Суб'єкти захисту об'єктів критичної інфраструктури*" в рамках бакалаврської програми спеціальності №081 "*Право*" як курс для самостійного вивчення студентами.

Пілотні програми формальної підготовки бакалаврів з питань захисту об'єктів критичної інфраструктури включають наступні напрями:

- Організаційно-правове забезпечення захисту інформації на об'єктах критичної інфраструктури;
- Правові основи організації та захисту об'єктів критичної інфраструктури;
- Кібербезпека об'єктів критичної інфраструктури;
- Системи безпеки об'єктів критичної інфраструктури;
- Автоматизовані системи відеоспостереження на об'єктах критичної інфраструктури;
- Електронний захист об'єктів критичної інфраструктури;
- Інспекційне обладнання на об'єктах критичної інфраструктури та інші.

Решта неліцензованих програм із ЗКІ пропонуються студентам університетів як факультативні навчальні програми, або окремими модулями, або як навчальні курси з підвищення кваліфікації фахівців із ЗКІ.

Українські університети та науково-дослідні установи налагодили добрі стосунки та співпрацю з університетами та навчальними центрами ЄС та США.

- У 1998 році в Інституті ядерних досліджень НАН України було відкрито Навчальний центр з фізичного захисту, обліку та контролю ядерного матеріалу імені Джорджа Кузмича. Створення навчального центру стало можливим завдяки фінансовій та технічній допомозі Міністерства енергетики США. З моменту заснування були розроблені та впроваджені різноманітні навчальні курси з фізичного захисту та контролю і обліку ядерних матеріалів (ФЗ та ОЯМ) як курси підвищення кваліфікації для спеціалістів з ФЗ та ОЯМ. В результаті діяльності Навчального центру до спеціальності №143 "*Атомна енергетика*" в ряді університетів України додано бакалаврську та магістерську програму "*Фізичний захист та облік і контроль ядерних матеріалів*".
- У 2016 році українські дослідники та науковці зі Східноукраїнського національного університету імені Володимира Даля та Херсонського національного технічного університету розробили пілотну версію магістерської програми "*Аналіз ризиків безпеки та стійкості* " в рамках проекту TEMPUS "*Модернізація післядипломної освіти з безпеки та*

стійкості для гуманітарних та промислових галузей". Основна мета програми полягала у створенні бази знань для міждисциплінарних досліджень з управління ризиками критичної інфраструктури та розробці навчальної програми з безпеки для відповідних і визнаних галузевих та академічних експертів. Очікувалося, що ця програма дозволить підготувати висококваліфікованих фахівців і озброїти їх сучасними інструментами і методами, які дозволять оцінювати ризики безпеки, управляти ризиками і реагувати на нові виклики кіберсуспільства. За результатами пілотної програми було розроблено окремий навчальний курс "*Кібербезпека об'єктів критичної інфраструктури*". Університет включив його до програми підготовки магістрів за спеціальністю №125 "*Кібербезпека*".

- Модулі "*Захист та стійкість критичної інфраструктури*" та "*Енергетична безпека*" включені до програми "*Стратегічне лідерство*": *Національна безпека*" магістерської програми з державного управління в секторі безпеки та оборони Києво-Могилянської бізнес-школи. Програма розроблена та впроваджується у партнерстві з Радою національної безпеки і оборони України та Офісом Президента України за підтримки міжнародних партнерів - США, Канади, Великої Британії, НАТО та українських місій.

У наведеній нижче таблиці ви можете побачити перелік українських університетів та навчальних центрів, які почали впроваджувати навчальні програми з ЗКІ у свій формальний та неформальний освітній процес для розвитку майбутніх кадрів ЗКІ в Україні.

Назва навчального закладу	Спеціальність	Тип програми	Назва навчальної програми
Національний авіаційний університет	№263 "Цивільний захист"	Ступінь бакалавра	Захист об'єктів критичної інфраструктури
Міжрегіональна академія управління персоналом	№081 "Право"	Ступінь бакалавра (*курс для самостійного навчання*)	Суб'єкти захисту об'єктів критичної інфраструктури
Національна академія Служби безпеки України, Навчально-науковий інститут державної безпеки	№256 "Національна безпека" *Кіберзахист, забезпечення державної безпеки в інформаційній сфері (ІС)*	Сертифікат про акредитацію освітньої програми відсутній (*факультативна навчальна програма*)	Контррозвідувальний захист кібербезпеки держави та об`єктів критичної інфраструктури
Національна академія Служби безпеки України, Навчально-науковий інститут державної безпеки	№256 "Національна безпека" *Забезпечення державної безпеки в інформаційній сфері*	Сертифікат про акредитацію освітньої програми відсутній (*факультативна навчальна програма*)	Контррозвідувальний захист кібербезпеки держави та об`єктів критичної інфраструктури

Назва навчального закладу	Спеціальність	Тип програми	Назва навчальної програми
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"	№143 "Атомна енергетика"	Ступінь магістра	Фізичний захист та облік і контроль ядерних матеріалів
Вінницький національний технічний університет	№125 "Кібербезпека"	Ступінь бакалавра і магістра	Кібербезпека критичної інфраструктури
Східноукраїнський національний університет імені Володимира Даля	№125 "Кібербезпека"	Ступінь бакалавра	Кібербезпека критичної інфраструктури
Бізнес-школа Києво-Могилянської академії		Магістр державного управління у сфері оборони та безпеки	Програма стратегічного лідерства: Курс "*Національна безпека*", модулі: - Захист та стійкість критичної інфраструктури; - Енергетична безпека.
Навчальний центр з фізичного захисту, обліку та контролю ядерного матеріалу імені Джорджа Кузмича Національної академії наук України, Інститут ядерних досліджень		кваліфікаційні програми підготовки та перепідготовки спеціалістів з ФЗ та ОЯМ ядерних установок	Фізичний захист (до навчальної програми включено 14 курсів) Контроль та облік ядерних матеріалів (до навчальної програми включено 14 курсів)

Сучасна підготовка здобувачів вищої освіти з питань ЗКІ спрямована на безперервний професійний та особитий розвиток з можливістю подальшої інтеграції в цивільну, безпекову та науково-дослідницьку сфери і, звичайно, вміння застосовувати отримані знання на ринку професійної діяльності у сфері ЗКІ. Якщо говорити про підготовку фахівців ЗКІ для сектору безпеки,

то основними замовниками освітніх послуг в Україні є Служба безпеки України; органи сектору безпеки та оборони; органи державної влади. До компетенцій таких фахівців належать контррозвідка, захист національної державності, боротьба з тероризмом та контррозвідувальний захист об'єктів критичної інфраструктури тощо.

Якщо розглядати компетенції спеціальності "Цивільний захист", то основним завданням фахівців з цивільного захисту є організація захисту критичної інфраструктури та території, забезпечення готовності до проведення ефективних заходів щодо захисту населення у надзвичайних ситуаціях техногенного та природного характеру.

Але всі згадані програми, курси та спеціальності не охоплюють весь спектр підготовки фахівців з ЗКІ, необхідних Україні на даний момент. Причиною цього є те, що ЗКІ досі не виділений як окрема професія або галузь знань у формальній освіті в Україні. Перешкодою для запровадження цієї критично важливої для України спеціальності є те, що Міжнародна стандартна класифікація освіти не виділяє сферу захисту критичної інфраструктури як окрему галузь знань чи професію. Запровадження спеціальності ЗКІ як окремої в сучасних українських правових реаліях суперечило б Закону України "Про вищу освіту" та міжнародним зобов'язанням України. Саме тому українські університети заповнюють цю прогалину, впроваджуючи цю галузь знань та її зміст через міждисциплінарні освітні програми в правоохоронних, оборонних та цивільних академіях. Водночас, цей правовий тягар та відсутність ЗКІ як окремого стандарту в класифікації ускладнює для викладачів українських університетів отримання схвалення їхніх програм з ЗКІ від Міністерства освіти і науки України (МОНУ) та отримання сертифікатів викладачів ЗКІ після пілотування їхніх поточних бакалаврських освітніх програм.

Для вирішення цієї проблеми Служба захисту критичної інфраструктури при Раді національної безпеки і оборони України (СЗКІ/РНБОУ) спільно з МОНУ та міжнародним партнером - CRDF Global в Україні - розробила проєкт Концепції розвитку системи підготовки фахівців з питань захисту критичної інфраструктури. Розробка Концепції стала особливо актуальною у зв'язку з прийняттям Закону України "Про критичну інфраструктуру" від 16 листопада 2021 року. Цей закон є основою для розвитку системи захисту критичної інфраструктури країни та містить положення, які, зокрема, передбачають розробку навчальних програм для здобувачів вищої освіти, програм підвищення кваліфікації, роботи та навчання працівників у сфері захисту критичної інфраструктури.

Метою Концепції є створення національної системи підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері захисту критичної інфраструктури для забезпечення потреб країни у фахівцях та підвищення рівня обізнаності, у тому числі просвітницької діяльності, всіх верств населення та його готовності до протидії безпековим викликам.

До початку російсько-української війни 24 лютого 2022 року Концепція була схвалена Кабінетом Міністрів України та направлена до Міністерства

освіти України та Міністерства економіки України для остаточного узгодження та розгляду. Очікується, що Концепція буде реалізована протягом 2023-2033років.

Відповідно до Концепції, план реалізації цієї ініціативи складається з 2 етапів:

- І етап (2023-2028 роки): розроблення кваліфікаційних вимог до персоналу із ЗКІ, реалізація пілотних короткострокових програм професійного розвитку персоналу, визначення вимог до освітніх програм (у тому числі міждисциплінарних) та науково-дослідної роботи щодо доповнення Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, новою позицією у сфері забезпечення стійкості та захисту критичної інфраструктури, та до 1 січня 2024 року поінформувати про результати Кабінет Міністрів України і подати проєкт відповідного рішення та пропозиції щодо програм навчання, підвищення кваліфікації, робочих і навчальних програм відповідно до 9 розділу "Прикінцеві та Перехідні положення" Закону України «Про критичну інфраструктуру» щодо формування компетентностей випускника, спроможного працювати у сфері ЗКІ, визначення опорних закладів вищої освіти для реалізації «пілотного проєкту» (за згодою ЗВО);

- ІІ етап (2028-2033 роки): забезпечення добору осіб та їх підготовка для набуття відповідних компетентностей у сфері ЗКІ, а також, після проведення пілоту, за результатами проведення науково-дослідної роботи щодо доповнення Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, за необхідності доповнити його новою позицією у сфері забезпечення стійкості та захисту критичної інфраструктури,; початок реалізації спеціалізованих освітніх програм формальної вищої освіти.

Вплив міжнародної допомоги на розробку навчальних планів та навчальних програм для академічних кіл ЗКІ.

Слід зазначити, що значний вплив на розвиток національних навчальних програм і навчальних планів з СІП в українських академічних колах, науково-дослідних установах та навчальних центрах мала підтримка міжнародних донорів, посольств та міжнародних програм Сполучених Штатів Америки (США), Великої Британії (Велика Британія), Європейського Союзу (ЄС), Організації з безпеки і співробітництва в Європі (ОБСЄ) та Організації Північноатлантичного Договору (НАТО).

Протягом останнього десятиліття міжнародними організаціями та експертами спільно з українськими державними установами, науковими колами та приватним бізнесом було проведено чимало міжнародних виїзних та онлайн семінарів/тренінгів, навчань, тренінгів, візитів міжнародних спікерів, міжнародних візитів з обміну досвідом та науково-практичних конференцій для українських державних установ, академічних кіл та приватного бізнесу.

- 5 практичних виїзних семінарів "*Захист критичної інфраструктури/ключових ресурсів*", Посольство США в Україні, офіс радника з питань професійної підготовки (ОРПП), Федеральний правоохоронний навчальний центр, Департамент внутрішньої безпеки США (ФНЦПО/ДВБ), 2010-2011 рр;
- *Національна конференція США з безпеки спорту*, Національний центр безпеки глядачів у спорті (NCS4), ФНЦПО/ДВБ, Державна прикордонна служба України (ДПСУ), Служба безпеки України (СБУ), Міністерство надзвичайних ситуацій України (МНС), 02-04 серпня 2011 р;
- Круглий стіл "Захист критичної інфраструктури: Проблеми та перспективи впровадження в Україні", Національний інститут стратегічних досліджень (НІСД) України, 17 липня 2012 р;
- Семінар "*Організаційні аспекти побудови системи захисту критичної інфраструктури в Україні*", Національний інститут стратегічних досліджень України (НІСД), Офіс зв'язку НАТО в Україні, 25 лютого 2016 р;
- Міжнародний семінар "*Захист критичної інфраструктури. Досвід європейських країн", Служба безпеки України, Організація з безпеки і співробітництва в Європі (ОБСЄ), 11-13 жовтня 2016 року;*
- *Семінар "Створення системи підготовки кадрів в Україні у сфері ЗКІ*", Національний інститут стратегічних досліджень України (НІСД), Програма НАТО з професійного розвитку (ППО) в Україні, 09 листопада 2016 р;
- Семінар "*Основні підходи до планування дій у разі виникнення кризових ситуацій на об'єктах критичної енергетичної інфраструктури*", Національний інститут стратегічних досліджень України (НІСД), 13 квітня 2017 р;
- Перша міжнародна науково-практична конференція "*Критична інфраструктура України як об'єкт кримінально-правової охорони та превентивної діяльності. Роль і місце спеціальних служб у державній системі захисту критичної інфраструктури, правові аспекти та основні завдання*", ОБСЄ, Служба безпеки України, Прикарпатський національний університет імені Василя Стефаника, 08-10 червня 2017 р;
- Семінар "*Критична національна інфраструктура*", Національний інститут стратегічних досліджень України (НІСД), Коледж планування на випадок надзвичайних ситуацій Кабінету Міністрів Великої Британії, 19-23 червня 2017 р;
- Семінар "Критична національна інфраструктура: Енергетичний сектор". НІСД, Коледж планування на випадок надзвичайних ситуацій при Кабінеті Міністрів Великої Британії, 04-07 вересня 2017 року;

- Командно-штабні навчання "*Непорушна стійкість - 2017*", Національний інститут стратегічних досліджень України (НІСД), Центр передового досвіду НАТО з енергетичної безпеки та Міністерство енергетики та вугільної промисловості України, Школа післядипломної освіти ВМС США, 16-20 жовтня 2017 р;
- Міжнародний круглий стіл "*Роль і місце спеціальних служб у захисті критичної інфраструктури*", Служба безпеки України, ОБСЄ, 29 листопада 2017 р;
- Друга міжнародна науково-практична конференція "*Становлення та перспективи розвитку державної системи захисту критичної інфраструктури в Україні. Кримінологічна оцінка ризиків та загроз*", ОБСЄ, Служба безпеки України, Прикарпатський національний університет імені Василя Стефаника 26-28 квітня 2018;
- Круглий стіл "*Сертифікація критичної інфраструктури: формування системи аналізу інформації*", Національний інститут стратегічних досліджень України (НІСД), Державна архівна служба України, 22 березня 2018 р;
- Курс кризового менеджменту з модулем "*Захист критичної інфраструктури*", Національна академія Національної гвардії України, Навчальна програма Україна-НАТО, Офіс зв'язку НАТО в Україні, НІСД, 29-31 травня 2018 р;
- Міжнародний круглий стіл "*Захист критичної інфраструктури та посилення хімічної безпеки на сході України*", візит в Україну колишнього заступника помічника міністра з питань захисту інфраструктури Міністерства внутрішньої безпеки США пана Девіда Вульфа, офіс Координатора проектів ОБСЄ в Україні, 16 серпня 2018 р;
- Командно-штабні навчання "*Непорушна стійкість - 2018*", Національна академія внутрішніх справ України, Посольство Великої Британії в Україні, 08-11 жовтня 2018 р;
- Міжнародний семінар "*Захист критичної інфраструктури. Досвід європейських країн*", ОБСЄ, НІСД, Міністерство транспорту України, 07-08 листопада 2018 р;
- Дев'ятий модуль "*Захист критичної інфраструктури*" в рамках проекту "*100 чемпіонів*", Програма розвитку НАТО, НАВС України, 12-13 листопада 2018 р;
- Міжвідомча робоча група експертів з питань протидії розповсюдженню зброї масового знищення, тероризму та захисту критичної інфраструктури на тему "Проблеми побудови державно-приватного партнерства у сфері захисту критичної інфраструктури", НІСД, 18 квітня 2019 р;
- Третя щорічна міжнародна науково-практична конференція "*Становлення та перспективи розвитку державної системи захисту критичної інфраструктури в Україні*", ОБСЄ, Служба

безпеки України, Прикарпатський національний університет імені Василя Стефаника, 12-14 вересня 2019 р;

- Онлайн-круглий стіл "*Вища освіта з кібербезпеки в Україні*", Агентство США з міжнародного розвитку (USAID), проєкт USAID "Кібербезпека критичної інфраструктури України", Харківський національний університет радіоелектроніки, 19 листопада 2020 р;
- Онлайн-семінар "*Створення нормативно-правової бази для забезпечення безпеки та стійкості критичної інфраструктури: попередні результати та пріоритети подальшої роботи*", НІСД, Місія НАТО в Україні, 25 лютого 2021 р;
- Національний кластер кібербезпеки "Захист критичної інфраструктури", CRDF Global в Україні, ДССЗЗІ/РНБО України, 27 травня 2021 р;
- Онлайн-семінар "Захист критичної інфраструктури", NextPeak, CRDF Global в Україні, ДССЗЗІ/РНБО України, 02-03 червня 2021 р;
- Командно-штабні навчання "Непорушна стійкість - 2020", Секретаріат КМУ, Центр передового досвіду НАТО з енергетичної безпеки, оборонні та правоохоронні органи України, НІСД, 13 -17 вересня 2021 р;
- Четверта щорічна міжнародна науково-практична конференція "Становлення та перспективи розвитку державної системи захисту критичної інфраструктури в Україні", ОБСЄ, СБУ та ДССЗЗІ/РНБО України, 28-30 жовтня 2021 р;
- Онлайн-семінар "Захист критичної інфраструктури", US Nouset National Security Group LCC, CRDF Global в Україні, ДССЗЗІ/РНБО України, 02-04 листопада 2021 р;
- Вебінар "Дослідження розвитку захисту критичної інфраструктури України", CRDF Global в Україні, ДССЗЗІ / РНБО України, 09 грудня 2021 р;
- Вебінар "Невідкладні дії: Зниження ризиків для сектору критичної інфраструктури в Україні.", Рада національної безпеки і оборони України (РНБО), Catalisto та CRDF Global, 14 листопада 2022 року;
- Практичний семінар "*Безпека та стійкість критичної інфраструктури*", ", CRDF Global в Україні, ДССЗЗІ / РНБО України, Польща, Варашава, 26-31 березня 1, 2023р;
- Командно-штабні навчання з кіберстійкості критичної інфраструктури Critical Infrastructure Resilience Exercises (CIREX), Агентство США з міжнародного розвитку (USAID), проєкт USAID "Кібербезпека критичної інфраструктури України", 20 квітня 2023 р;
- Практичний семінар з питань створення та функціонування національної системи захисту критичної інфраструктури (ЗКІ) в Україні, CRDF Global, Державна служба спеціального зв'язку та захисту інформації України, Департмент захисту критичної інфраструктури, 23 травня 2023 р.

Навчання та освіта мають фундаментальне значення для успіху національної програми розвитку безпеки та стійкості критичної інфраструктури в Україні і повинні продовжувати охоплювати державних службовців, власників та операторів інфраструктури, служби швидкого реагування та громадськість, де це доречно. Навчання повинно бути доступним у різних формах для забезпечення якнайширшого охоплення на основі найкращих практик США, Великої Британії, НАТО та ЄС.

Створення культури постійного вдосконалення безпеки і стійкості інфраструктури вимагає також збільшення уваги до фундаментальних концепцій у певних навчальних програмах коледжів і університетів. Метою академічних програм може бути: навчити студентів використовувати методи оцінки; підвищити обізнаність інженерів про способи захисту елементів інфраструктури, зменшення їх вразливості або підвищення стійкості за рахунок проектування; інформувати планувальників про важливість завчасного планування, обміну інформацією і партнерства; допомогти менеджерам з надзвичайних ситуацій зрозуміти потенційний вплив каскадних збоїв; серед інших факторів.

Висновки. Побудова національної системи підготовки фахівців з ЗКІ та навчальних програм потребуватиме багато часу та роботи в Україні спільно з міжнародними експертами та провідними міжнародними освітніми/дослідницькими установами у підготовці національної команди викладачів, розробці національних навчальних програм з ЗКІ, програм електронного навчання, тренінгів на робочому місці, навчальних посібників тощо, а також проведення великої кількості пілотних проєктів з академічними колами та спільнотою ЗКІ до їх інтеграції в освітній процес.

1. Бізнес-школа Києво-Могилянської академії, магістерська програма з державного управління у сфері оборони та безпеки. Отримано з https://slp.kmbs.ua/en [Доступно 2 червня 2022].
2. Верховна Рада України (2014), Закон України "Про вищу освіту" № 37-38. Отримано з https://zakon.rada.gov.ua/laws/show/1556-18#top [Доступно 16 травня 2022 р.].
3. Навчальний центр з фізичного захисту, контролю та обліку ядерного матеріалу ім. Джорджа Кузмича (1998), Каталог курсу. Отримано з http://www.mpca.kiev.ua/doc/Course_cataloque_ua.pdf [Доступно 3 червня 2022].
4. Національна академія Служби безпеки України, Каталог освітніх програм [Електронний ресурс]. Отримано з https://registry.edbo.gov.ua/university/1339/study-programs/ [Доступно 1 червня 2022 р.].
5. Міжрегіональна академія управління персоналом, Освітня програма, Суб'єкти захисту об'єктів критичної інфраструктури для бакалаврів https://maup.com.ua/ua/navchannya-u-maup/library/metod/12-pravo/navchalna_programa_disciplini_sub_ekti_zahistu_ob_ektiv_kritichnoi_infrastrukturi_dlya_bakalavriv.html [Доступно 15 травня 2022 р.].
6. Міністерство освіти і науки України (2018), Наказ Міністерства освіти і науки України №1074 від 4 листопада 2018 року "Про затвердження Стандарту вищої освіти за спеціальністю 125 "Кібербезпека" для першого (бакалаврського) рівня

освіти". Отримано з https://mon.gov.ua/storage/app/uploads/public/5bb/626/1a8/5bb6261a8477616640916 4.pdf [Доступно 26 травня 2022 р.].

7. Міністерство освіти і науки України (2018), Наказ Вінницького технічного університету № 4 від 11 листопада 2018 року "Про затвердження освітньо-професійної програми "Кібербезпека критичних систем" за першим (бакалаврським) рівнем освіти" для спеціальності № 125 "Кібербезпека [Електронний ресурс]. Отримано з https://vntu.edu.ua/images/docs/2019/fitki/4.pdf [Доступно 1 червня 2022 р.].
8. Міністерство освіти і науки України (2021), Наказ Міністерства освіти і науки України № 332 від 18 березня 2021 року "Про затвердження Стандарту вищої освіти за спеціальністю 125 "Кібербезпека" за другим (магістерським) рівнем освіти". Отримано з https://mon.gov.ua/storage/app/media/vyshcha/ standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx [Доступно 3 червня 2022 р.].
9. Міністерство освіти і науки України (2021), Наказ Національного авіаційного університету, від 1 червня 2021 р. Про затвердження освітньо-професійної програми "Захист об'єктів критичної інфраструктури" за першим (бакалаврським) рівнем спеціальності № 263 "Цивільний захист" [Електронний ресурс]. Отримано з https://nau.edu.ua/download/ Quality20Assurance_ukr/Projekti/_compressed.pdf [Доступно 1 червня 2022 р.].
10. Міністерство освіти і науки України (2021), Наказ Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" №НОН/89/2021 від 1 червня 2021 року Про затвердження освітньо-професійної програми "Фізичний захист та облік і контроль ядерних матеріалів" за другим (магістерським) рівнем спеціальності № 143 "Фізична ядерна безпека". Отримано з https://osvita.kpi.ua/sites/default/files/opfiles/143_OPPM_FZOKYaM_2021.pdf [Доступно 3 червня 2022 р.].
11. Рада національної безпеки і оборони України (2020), Розпорядження Ради національної безпеки і оборони України №64 від 13 серпня 2020 року "Про проект рішення Ради національної безпеки і оборони України "Про Концепцію розвитку системи підготовки фахівців з питань захисту критичної інфраструктури". Отримано з робочого проєкту [Доступно 16 травня 2022 р.].
12. Рада національної безпеки і оборони України (2021), новини Ради національної безпеки і оборони України, Фахівці Апарату РНБО України взяли участь в онлайн-семінарі з питань захисту критичної інфраструктури [Українською мовою], отримано з https://www.rnbo.gov.ua/en/Diialnist/5124.html [Доступно 27 травня 2022 р.].
13. Рада національної безпеки і оборони України (2021), новини Ради національної безпеки і оборони України, Апарат РНБО провів перший в Україні семінар для представників обласних державних адміністрацій з питань захисту критичної інфраструктури [Українською мовою]. https://www.rnbo.gov.ua/ en/Diialnist/4910.html [Доступно 25 травня 2022 р.].
14. Центр адаптації державної служби до стандартів Європейського Союзу, Дев'ятий модуль "Захист критичної інфраструктури" в рамках проекту "100 чемпіонів" [Електронний ресурс]. Отримано з http://www.center.gov.ua/prestsentr/novini/item/3237 [Доступно 23 травня 2022 р.].

15. Information & Security: An International Journal (2016), Skarga-Bandurova, Ryazantsev, and Kiryushatova, vol.35, no. 2, 2016, 123-132, Retrieved from https://doi.org/10.11610/isij.3506 [Accessed 13 May 2022]
16. International Standard Classification of Education (ISCED) http://uis.unesco.org/en/topic/international-standard-classification-education-isced [Accessed 11 May 2022].
17. Sukhodolia, O., Walzer L. (2022). NATO Tabletop Exercises to Further Energy Resilience and Security: Ukraine as a Case Study. The Combating Terrorism Exchange, Vol.12 №1, April 2022, pp. 16-25. Retrieved from https://nps.edu/documents/110773463/135759179/CTX-VOL1201-vFinal.pdf/dc7833e2-680d-400a-1430-a6c0a7fd09c6?t=1650471163152#page=17 [Accessed 30 May 2022] .
18. Sukhodolia, O. (2018), Training as a Tool of Fostering a CIP Concept Implementation: Results of a Table Top Exercise on Critical Energy Infrastructure Resilience. Information & Security: An International Journal vol.40, no. 2 (2018). Retrieved from https://infosec-journal.com/article/training-tool-fostering-cip-concept-implementation-results-table-top-exercise-critical [Accessed 25 May 2020].
19. Report (2021), Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education, ENISA, 21 June 2021 Retrieved from https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education [Accessed 22 May 2022].

В.А. Євдокімов

ДЕЦЕНТРАЛІЗАЦІЯ РИНКУ, ЯК ОСНОВА ПОБУДОВИ РЕЗИЛЬЄНТНОЇ ЕНЕРГОСИСТЕМИ УКРАЇНИ

Енергосистема України сьогодні працює в нових воєнних умовах, при якому безпека постачання є одною із головних критеріїв роботи. При цьому, в першу чергу, забезпечується електроенергією населення та підприємства, що забезпечують життєдіяльність регіонів. Це підприємства житлово-комунального господарства, транспорт та інші регіональні підприємства, що здійснюють постачання продуктів харчування для населення. Тому постає питання, яким чином забезпечити це, в умовах постійного цілеспрямованого руйнування об'єктів критичної інфраструктури та існуючої організаційно-технічної системи управління енергоринку.

Існуюча організаційно-технічна система управління енергоринку побудована за принципом централізації процесу виробництва, передачі, розділу та постачання електричної енергії споживачам, тобто зверху-вниз. Такий дизайн ринку притаманний не тільки в Україні, але і у всій Європі. Такий підхід не дозволяє в повній мірі вирішувати питання забезпечення надійного, безпечного та доступного за цінами, постачання електроенергії кінцевим споживачам, а також не дозволив залучити достатніх інвестиційній у будівництва нових маневрових потужностей. Тому потребує питання перегляду моделі ринку електроенергії, який би забезпечував та надавав правильні ринкові сигнали на забезпечення більш «жорсткої стійкості» енергетичного сектора[1], а також нових принципів адаптивного управління, планування та технічних рішень, тобто стати більш резильєнтної [2].

Проектування ринку електроенергії є одним з основних інструментів Європейського Союзу для ефективного переходу до кліматично нейтральної енергетичної системи, яка залежить від чистої електроенергії. Правильно спроектовані ринки електроенергії можуть стимулювати впровадження екологічно чистих енергетичних технологій, включаючи потужності відновлюваних джерел енергії, та гнучкі модульні станції, необхідні для їх підтримки, тим самим зберігаючи безпеку постачання [3]. Окрім цього, на сьогодні постає питання при проектуванні дизайну ринку електричної енергії враховувати дії в умовах мілітарного впливу (гібридних воїн), коли на енергетичну систему здійснюється цілеспрямовані удари на руйнування об'єктів енергетики. Проектування ринку також може допомогти забезпечити ефективну та безпечну роботу системи електропостачання, яка дедалі більше ставатиме основою декарбонізованої економіки. Крім того, ринки електроенергії можуть допомогти справедливо розподілити витрати та вигоди системи електропостачання.

Наша енергосистема радикально змінюється внаслідок декарбонізації. При цьому, система електропостачання стає більш децентралізованою, за рахунок підключення до локальних мереж відновлювальних джерел енергії

та діджиталізованою з боку активного попиту на рівні споживання електричної енергії. Це все створює проблеми на існуючому централізованому рівні, що підтверджується великими боргами з боку оператора системи передачі НЕК Укренерго перед Гарантованим постачальником та обмеженням виробництва електричної енергії з відновлювальних джерел енергії.

Стратегічною ціллю побудови ринку електричної енергії є вуглецева нейтральність, яка досягається розвитком чистої децентралізованої електричної енергії. Але в сьогоднішніх реаліях, коли здійснюються масові цілеспрямовані удари на об'єкти енергетики в умовах гібридної війни, постає питання протистояння та швидкого відновлення електропостачання після таких ударів. Тому, при проектування ринку електричної енергії необхідно враховувати не тільки фактори природнього чи техногенного характеру, але і загроз гібридного характеру, які можуть спричинити все, від перебоїв у електропостачанні до хронічного недопостачання електричної енергії.

Децентралізація направлена на взаємовідносин на локальному рівні – на рівні взаємодії між виробником електричної енергії, якій приєднаний до розподільчих мереж, або активного споживача, який має надлишок енергії, якій також віддається у розподільчу мережу та учасниками роздрібного ринку, а саме оператором системи розподілу, постачальником та постачальником універсальних послуг. Тобто, технологічно вироблена електрична енергія в межах локальної (розподільчої) мережі споживається споживачами цієї ж самої мережі. Таким чином, побудова децентралізованого ринку повинна враховувати технологічні особливості виробництва та споживання електричної енергії в локальній (розподільчій) мережі, а також забезпечувати надійність та безпековість постачання, особливо в умовах мілітарного впливу (гібридної війни). Це можливо реалізувати шляхом проведення реформації існуючої централізованої енергетичної системи вертикального управління, у дворівневу систему управління – горизонтально-вертикальну, тобто знизу-у верх. Це можливо забезпечити за рахунок зближення ринкових взаємовідносин виробника електричної енергії із альтернативних джерел енергії, які приєднані до локальних (розподільчий мережах) з кінцевими споживачами, які забезпечують життєдіяльність регіонів. І таким чином, забезпечується резильєнтність енергетичної системи, а також створюються передумови по залученню інвестицій до регіонів, і як наслідок збільшення інвестиційної привабливості та капіталізації регіонів.

Висновок

Необхідно продовжувати здійснювати вдосконалення дизайну енергоринку шляхом поступового поетапного переходу від централізованої системи управління до частково децентралізованої, а також розвитку нових ринкових правил роздрібного ринку, яка направлена на забезпечення електроенергією населення та підприємства, що забезпечують життєдіяльність регіонів за справедливими цінами та доступністю. Це в свою

чергу, дозволить розпочати побудову нової резильєнтної енергосистеми України, а також зміни механізмів підтримки зеленої генерації.

1. Саух С.Є. Концепція побудови жорсткої резильєнтної електроенергетичної системи України. – Збірник матеріалів конференції. - Наукова-технічна конференція молодих вчених та спеціалістів ІПМЕ. – 2023. – ст.137. https://ipme.kiev.ua/wp-content/uploads/2023/05/Матеріали-конференції-2023.pdf.
2. Stout S., Lee N., Cox S., Elsworth J., Leisch J. Power sector resilience planning guidebook. – U.S. Department of Energy's NREL and USAID. – 2019. – 82 p. – URL https://www.nrel.gov/docs/fy19osti/73489.pdf.
3. Georg Zachmann., Conall Heussaff. Phased European Union electricity market reform. - https://www.bruegel.org/policy-brief/phased-european-union-electricity-market-reform.

В.В. Мохор, Ф.О. Коробейніков, О.М. Дибач, О.О. Бакалинський

ВТІЛЕННЯ ПАРАДИГМИ РЕЗИЛЬЄНТНОСТІ В ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЄС

Парадигма резильєнтності поступово приходить на зміну парадигмі захисту, що явно простежується у спеціальних публікаціях NIST [1], публікаціях MITRE [2] і в розробленні стандартів ISO [3]. На загальному рівні це також знаходить своє відображення в останніх директивах Ради ЄС, що визначають нові пріоритети в забезпеченні безпеки об'єктів критичної інфраструктури [4].

В цьому контексті актуальним є порівняння цілей, задач і методів забезпечення резильєнтності, рівнів її імплементації та сфер застосування в директивах та рекомендаціях Ради ЄС, зокрема це Директива 2022/2557 від 14 грудня 2022 року щодо резильєнтності критично важливих об’єктів [5]; Директива 2022/2555 від 14 грудня 2022 року про заходи для забезпечення високого спільного рівня кібербезпеки в ЄС [6]; Рекомендації 2023/С 20/01 щодо загальноєвропейського скоординованого підходу до посилення резильєнтності критичної інфраструктури від 8 грудня 2022 року [7], з тими, що визначаються документами [1-3].

Перехід від концепції захисту до резильентності в ЄС, перш за все, підтверджується тим, що директива 2022/2557 скасовує попередню Директиву 008/114/ЄС від 8 грудня 2008 року про ідентифікацію та визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту [8], у зв'язку з твердженням авторів документу, "що через дедалі більш взаємопов'язаний та транскордонний характер операцій з використанням критично важливої інфраструктури захисних заходів, що стосуються лише окремих активів, недостатньо для запобігання усім збоям" [5].

Перехід ЄС до резильентності замість захисту зумовлений "динамічним ландшафтом загроз, який містить у собі гібридні та терористичні загрози, що розвиваються, а також зростаючу взаємозалежність між інфраструктурою та секторами. Крім того, існує підвищений фізичний ризик через стихійні лиха і зміну клімату, що збільшує частоту і масштаби екстремальних погодних явищ, які можуть знизити пропускну здатність, ефективність і термін служби певних типів інфраструктури." [5]

У цьому ж документі (вперше в європейських документах такого рівня) наводиться визначення поняття "резильєнтність". Директива визначає його як "здатність критичного об'єкта запобігати, захищати, реагувати, чинити опір,

пом'якшувати наслідки, поглинати, пристосовуватися і відновлюватися після інциденту". [6]

ЄС запроваджує резильєнтність критичних об'єктів на наднаціональному рівні, через Комісію, на яку покладено повноваження з реалізації директив [5], та Групи із забезпечення резильентності критичних об'єктів, яка складається з представників держав-членів ЄС та Комісії, і має підтримувати Комісію, сприяти співпраці між членами ЄС, та обміну інформацією з питань, що стосуються впровадженню резильентності [5].

Однак, слід зазначити, що ЄС відмовляється від створення власної спільної стратегії підвищення резильентності критично важливих об'єктів Союзу, зобов'язавши кожну державу-члена ЄС розробити й ухвалити таку стратегію самостійно до 17 січня 2026 року [4]. На держави-члени також покладається обов'язок самостійно ідентифікувати об'єкти критичної інфраструктури та здійснювати їхню підтримку. Крім того, ЄС делегує національним операторам критичної інфраструктури самостійне проведення аналізу ризиків своїх об'єктів та здійснення заходів, спрямованих на забезпечення їхньої резильєнтності. Це дещо суперечить парадигмі резильентності, описаній в чинних стандартах, згідно з якою, визначення критичних активів організації є прерогативою її керівного органу, так само як і аналіз ризиків, пов'язаних з забезпеченням організацією своїх основних функцій.

Попри те, що директиви ЄС віддають основні інструменти імплементації резильентності до рук держав-учасниць, і покладають на них відповідальність за забезпечення безпеки об'єктів критичної інфраструктури, директиви містять в собі методи резильєнтності і покликані посилити роль Союзу через скоординований захист, контекстуальну обізнаність, розробку методологій і створення дієвих механізмів адаптивного реагування на інциденти.

Так, згідно з директивою (ЄС) 2022/2555, "опрацювання інцидентів покладається на CSIRT, мережа яких має сприяти швидкій та ефективній оперативній співпраці між державами-членами" [4]. Передбачається створення єдиного Фреймворку реагування на інциденти (Cybersecurity Crisis Response Framework), що переросли в кризи та мають транскордонний характер. Директива встановлює багатоетапний підхід до повідомлення про значні інциденти, визначає термін, протягом якого організації повинні надавати попередження (24 години) і повідомлення (72 години) про серйозний інцидент.

Директива, також, містить описи нових підходів до захисту інформаційних активів, які можна охарактеризувати як резильєнтні.

По-перше, це прийняття необхідності підготовки до протидії загрозам із малоймовірними ризиками, реалізація яких може призвести до значних

---

6 'resilience' means a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident;

наслідків [4]. Це винятково новий, суто резильєнтний підхід до аналізу ризиків, який докорінно відрізняється від донині усталеного.

По-друге, державам-членам пропонується "просувати використання програмного забезпечення з відкритим вихідним кодом і відкритих стандартів шляхом проведення політики, що стосується використання відкритих даних і відкритого вихідного коду в рамках забезпечення безпеки за допомогою прозорості" [4]. Відкритість коду є тим фактором, який знижує ризики шляхом синергії його користувачів, що також є резильєнтним підходом.

По-третє, "в рамках своїх національних стратегій кібербезпеки держави-члени повинні прийняти політику заохочення активного кіберзахисту в рамках більш широкої оборонної стратегії" [4]. Це вкрай важливий з погляду кіберрезильєнтності пункт, який, за належної уваги з боку держави, може ознаменувати собою нову епоху в захисті об'єктів критичної інфраструктури.

Нові директиви велику увагу приділяють обміну знаннями та передовим досвідом, для цього ЄС пропонує країнам-учасницям "просувати політику, що лежить в основі створення державно-приватних партнерств[7], пов'язаних з кібербезпекою. Крім того, наголошується на необхідності створення "європейської бази вразливостей, в якій організації та постачальники мережевих та інформаційних систем, а також компетентні органи та CSIRT, зможуть розкривати та реєструвати на добровільних засадах загальновідомі вразливості з метою надання користувачам можливості вжити відповідних заходів щодо їх усунення" [4].

Рекомендації 2023/С 20/01 хоч і не мають обов'язкової сили, проте об'єднують розглянуті вище директиви в єдине ціле, визначаючи резильєнтність основним підходом у забезпечення безпеки критичної інфраструктури Євросоюзу [5]. В них описується низка цілеспрямованих дій на рівні ЄС і на національному рівні для підтримки та підвищення резильєнтності критично важливої інфраструктури з акцентом на ті з них, що має важливе транскордонне значення. Ці цілеспрямовані дії складаються з підвищеної готовності, посиленого реагування та міжнародного співробітництва.

Висновки

Ґрунтуючись на огляді директив і рекомендацій Євросоюзу щодо резильентності критичної інфраструктури та кібербезпеки, можна виділити декілька ключових моментів, що визначають стратегічний напрямок гарантування безпеки на рівні ЄС і держав-членів.

1. У зв'язку з неефективністю старих підходів, розроблено новий механізм гарантування безпеки об'єктів критичної інфраструктури ЄС, шляхом створення на базі Єврокомісії структури, яка контролює облік та аналіз ризиків критичних активів країн-учасниць.

---

[7] Public-private partnerships

2. Розроблено нові механізми взаємодії між Комісією та країнами-учасницями, покликані забезпечити більш ефективну співпрацю з метою захисту критичної інфраструктури від широкого спектра загроз.

3. Створено нові практики, спрямовані на запобігання та спільну ліквідацію наслідків інцидентів на об'єктах критичної інфраструктури, особливо тих, які мають транснаціональне значення.

4. Наголошено важливість резильєнтності як центрального підходу в забезпеченні безпеки об'єктів критичної інфраструктури ЄС. Однак, резильєнтність, втілена на рівні ЄС, ***має гарантувати безперервність критичних процесів Євросоюзу в цілому***, визначається директивами як здатність ***окремих критичних об'єктів*** держав-членів ЄС запобігати, захищати, реагувати, чинити опір, пом'якшувати наслідки, поглинати, пристосовуватися та відновлюватися після інциденту.

Це суперечить парадигмі резильєнтності, викладеній в існуючих стандартах і практиках [1-3], і знижує ефективність заходів ЄС, що може бути подолане подальшим розвитком нормативної бази та поглибленням наукових досліджень в сфері резильєнтності.

1. NIST Special Publication 800-160, Volume 2. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
2. MITRE. Cyber Resiliency Engineering Framework. Deborah J. Bodeau & Richard Graubart. https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf
3. ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes https://www.iso.org/obp/ui/#iso:std:iso:22316:ed-1:v1:en
4. Стійкість критичної інфраструктури ЄС: посилення політики та координації. Олександр Суходоля. https://niss.gov.ua/sites/default/files/2023-02/az_eu-cip-coordinated_24022023.pdf
5. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1686557595058
6. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1686557550927
7. COUNCIL RECOMMENDATION of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H0120%2801%29
8. ДИРЕКТИВА РАДИ 2008/114/ЄС від 8 грудня 2008 року https://zakon.rada.gov.ua/laws/show/984_002-08#Text

М.М. Худинцев, О.А. Хоменко

МЕТОДОЛОГІЧНІ ЗАСАДИ ІНДЕКСУ КІБЕРРЕЗИЛЬЄНТНОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кіберстійкість (кібервідмовостійкість, кіберрезильєнтність) – здатність організації долати будь-які стреси, збої, небезпеки та загрози для своїх кіберресурсів всередині організації та її екосистеми для впевненого виконання своєї місії та підтримки бажаного спосіб роботи.

Центр кібербезпеки Всесвітнього економічного форуму у співпраці з робочою групою Індексу кіберстійкості та в партнерстві з компанією Accenture розробив глобальний Індекс кіберстійкості (CRI) [1,2]. CRI надає керівникам організацій державного та приватного секторів спільну структуру кращих практик для впровадження кіберстійкості, а також механізм вимірювання ефективності та цінностей організації. CRI також є універсальним засобом оцінки та міжпартнерської взаємодії у цифрових екосистемах. Адаптація методології CRI для потреб галузей економіки (секторів критичної інфраструктури) та окремих корпоративних користувачів є актуальною та важливою проблемою підвищення рівня захищеності даних та суспільно важливих сервісів.

Основні компоненти моделі CRI:

- усталені практики кіберстійкості / Cyber Resilience Framework (CRF);
- індексування стану кіберстійкості / Cyber Resilience Index (CRI).

Таблиця 1 – Принципи, практики та субпрактики у моделі CRI

Принципи	
Практика	Субпрактика
Принцип 1. Регулярна оцінка та визначення пріоритетів кіберризиків	
Визначте контекст ризику, оцініть і визначте пріоритети	Карта основних екосистем і взаємозалежностей ланцюга постачання
	Зовнішній звіт про стан аналізу взаємозалежності кіберстійкості та пов'язані з нею зусилля з управління (≥ 1раз/1 рік)
Перевірка інтеграції ризиків	Кількісна оцінка ризиків, включно з кібернзагрозами та кібернебезпечністю (≥ 1раз/1 рік)
	Врахування результатів оцінки кіберризиків у рішення щодо бюджету та ресурсів
Прийняття рішень, заснованих на оцінці ризиків	Механізм внутрішнього звітування та наявність чітких каналів ескалації
	Аналізує керівництвом інцидентів і серйозних порушень, прийняття коригуючих рішень, проведення навчання

Принцип 2. Встановлення і підтримка основних заходів безпеки	
Використовуйте усталені практики та галузеві стандарти	Оцінка організації за визнаною національною або міжнародною системою безпеки (NIST 800-53, ISO 27001, інші, ≥ 1раз/1 рік)
	Перевірка організації на відповідність галузевим нормативним стандартам щодо безпеки, стійкості та конфіденційності (≥ 1раз/1 рік)
Зосередьтеся на критичних активах і операціях	Класифікація активів та операцій (звичайні, критичні та/або базові)
	Ведення реєстру управління активами та операціями
Зменшуйте вплив загроз	Дотримання правил (принципів) зменшення негативного впливу загроз
	IT- та ІБ-архітектура обмежують каскадний та комплексний вплив
Вимірюйте зрілість та ефективність	Визначення та централізоване відстеження набору показників зрілості та продуктивності
	Звіти керівництву про визначені показники безпеки та тенденції щодо кіберстійкості (≥ 1раз/3 міс.)
Стимулюйте постійне вдосконалення	План дій щодо ініціатив з покращення, (оновлення ≥ 1раз/1 рік)
	Звіти керівництву про ефективність у порівнянні з критеріями успіху для реалізації ініціатив щодо вдосконалення плану дій (≥ 1раз/3 міс.)
Інтеграція реакції та відновлення	Відстеження економічної результативності заходів реагування та відновлення за допомогою показників, постійно оновлення базових показників
	Регулярний перегляд базових показників з корегуванням плану дій
Принцип 3. Включення управління кіберстійкістю у бізнес-стратегію	
Інститут управління кіберстійкістю	Встановлена структуру управління кіберстійкістю, організаційна схема, операційна модель, ролі щодо підзвітності та відповідальності
	Стратегія кіберстійкості, принципи стійкості; кодифікована міждисциплінарна співпраця, взаємодії та практики, чинні політики
Наглядова рада за кіберстійкістю	Задокументованість відповідальності за встановлення допустимих рівнів ризику стійкості, управління впливом і додавання цінності організації через стійкість
	Регулярні брифінги про стан кіберстійкості з дорученнями керівництву організації
Призначте відповідальну	Формальне визначення та задокументованість ролі з чітко зрозумілими очікуваннями та зобов’язаннями

посадову особу	Механізми надання відповідальній посадовій особі вільного доступу до ради директорів, розширення повноважень щодо стратегії кіберстійкості, управління та примусових дій, навчання керівників, придбання кадрових, фінансових і технологічних ресурсів
Принцип 4. Заохочення системної стійкості і співпраці	
Заслужіть довіру через підзвітність і прозорість	Відповідальність і підзвітність за агрегування та передачу третім сторонам практики забезпечення кіберзахищеності покладено на окрему роль або групу
	Порівняльний аналіз кіберстійкості та огляди передового досвіду з ключовими партнерами екосистеми
Сприяння співпраці в масштабах екосистеми	Угоди про обмін інформацією з ключовими партнерами екосистеми з питань кіберстійкості
	Чіткі очікування щодо того, що можна, а що не можна спільно використовувати
Поліпшення можливостей кіберстійкості екосистеми	Ланцюжок створення вартості кіберстійкості та розуміння ролі, критичності і залежності себе та кожного суб'єкта у екосистемі
	Участь у робочих групах, комітетах із розробки стандартів, галузевих асоціаціях та інших форумах співпраці
Принцип 5. Переконайтеся, що дизайн підтримує кібервідмовостійкість	
Сприяти стійкості за проектом	Принципи та цілі для стійкої архітектури команд, процесів і технологічних активів, дотримання принципу найменшого впливу для зменшення площини атак
	Перевірка команд, процесів, технологій та взаємопов'язаних систем на відповідність принципам і цілям стійкості (≥ 1раз/1 рік або під час створення)
Оптимізуйте всі функції	Ревізія процесів і активів управління кіберстійкостю (підрозділи ІБ-, ІТ-, інженерія, експлуатація сайту, бізнес-підрозділи, ≥ 1раз/1 рік)
	Розробка сценаріїв стійкості шляхом співпраці з усіма зацікавленими сторонами. Навчання щодо стійкості та стрес-тести (≥ 1раз/1 рік). Можливості для вдосконалення задокументовані та включені у стратегію стійкості та операційні процедури
Перевіряйте скомпрометовані ресурси	Планування та очікування продуктивності враховують можливість нерегулярних та руйнівних подій
	Відстеження показників нерегулярних вхідних даних і руйнівних подій
Інновації для майбутнього	Ресурси на дослідження, розробки та інноваційні ініціативи
	Постійне фінансування та активне управління цих заходів як частина бюджетного процесу

Принцип 6. Розвиток культури стійкості	
Сприяти обізнаному лідерству	Цілі керівництва щодо продуктивності роботи, пов’язані з ефективністю кіберстійкості
	Наймання керівництва з досвідом роботи з питань кіберзахисту та стійкості
Стимулюйте культуру через лідерство	Визначені, задокументовані та повідомлені винагороди, критерії успіху, покарання, наслідки та заходи для коригувальних дій для всіх працівників, пов’язаних із кіберстійкою поведінкою, що підкріплюються регулярним навчанням
	Демонстрація культури кіберстійкості з боку керівництва
Заслужіть довіру завдяки підзвітності та прозорості	Вимірювання та відстежування показників для оцінки культури стійкості, прозорості та підзвітності
	Регулярне інформування працівників про стан культури кіберстійкості, прозорості та підзвітності
Чемпіонат поведінки співробітників	Регулярні тренінги з кіберстійкості для всіх працівників
	Наявність цілей ефективності роботи, пов’язані зі сприянням позитивній стійкій до кібернетичної поведінки
Забезпечте безперервне навчання	Постійне навчання для критично важливих посад
	Активній формат тренінгів, навчань, курсів

1. The Cyber Resilience Index: Advancing Organizational Cyber Resilience, White Paper World Economic Forum, July 2022, 29 p.
2. Худинцев М.М., Жилін А.В., Давидюк А.В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог). Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. К.: 2021. 240 с.

О.Г. Додонов, О.С. Горбачик, М.Г. Кузнєцова

ІНФОРМАЦІЙНІ СИСТЕМИ І ЖИВУЧІСТЬ КРИТИЧНИХ ІНФРАСТРУКТУР

Критичні інфраструктури є життєво важливими для функціонування, безпеки та сталого розвитку сучасного суспільства, тому необхідно забезпечити такий стан інфраструктури, коли ризик нанесення шкоди людині, суспільству, країні скорочується до прийнятного рівня. Живучість, як здатність зберігати свою функціональність та відновлюватися після природних катастроф, терористичних актів, кібератак, технічних збоїв, стає необхідною властивістю критичної інфраструктури.

Внаслідок масштабної автоматизації та інформатизації управлінських та технологічних процесів до складу критичних інфраструктур входять інформаційні системи (ІС) різних рівнів, зокрема, експлуатаційного рівня об'єктів критичної інфраструктури, ІС рівня знань, ІС рівня управління, інформаційно-аналітичні системи стратегічного рівня. ІС критичних інфраструктур орієнтовані на роботу з інформацією й інтенсивний обмін даними в умовах фактичного злиття автоматизованого виробництва, виробничих технологій з мінімальним передбаченим втручанням людини у технологічні й управлінські процеси, які необхідні в нормальних умовах функціонування критичної інфраструктури, а також на забезпечення оперативного й ефективного управління критичними інфраструктурами в умовах загроз і небезпек.

ІС у загальному випадку являють собою сукупність засобів і методів пошуку, збору, збереження, оброблення і надання інформації користувачам для досягнення визначеної мети. Складовими ІС є програмні і апаратні засоби, організаційне забезпечення, регламенти і норми експлуатації, персонал, задіяний у процесах управління і адміністрування всіх компонентів ІС, та дані, якими управляє система. Від якості функціонування ІС залежить функціональність, надійність і безпека критичних об'єктів та інфраструктур. Наслідки відмов апаратних, програмних і комунікаційних засобів ІС можуть бути значущими не лише для самих критичних інфраструктур, а й для навколишнього середовища, життя і здоров'я людей, тому важливим є розуміння функціональності ІС критичних інфраструктур та забезпечення вимог до їх функціональної стійкості.

ІС експлуатаційного рівня забезпечують операційне оброблення даних і управління виробничими процесами на об'єктах критичної інфраструктури. Системи рівня знань та рівня управління (ІС менеджменту середньої ланку) орієнтовані на моніторинг стану критичної інфраструктури і окремих об'єктів, контроль, напрацювання й прийняття управлінських рішень, адміністрування тощо. Засоби цих ІС дозволяють відслідковувати і порівнювати поточні показники функціонування інфраструктури з минулими, архівувати і забезпечувати доступ до архівної інформації,

складати звіти за певний час і т. ін. ІС стратегічного рівня задіяні у довгостроковому планування, аналізі і прогнозуванні змін середовища функціонування об'єктів критичної інфраструктури, аналізі ризиків, прогнозуванні потенційних загроз, виявленні уразливостей в критичних інфраструктурах, а також визначенні ресурсів для відновлення критичної інфраструктури в умовах надзвичайної ситуації.

Для ІС завжди існує загроза деструктивних впливів із зовнішнього середовища, через дії персоналу чи конструктивні дефекти апаратних чи програмних засобів, відмови технічних засобів, через недостовірність, неточність чи недостатність даних в інформаційних ресурсах системи, що може призвести до неможливості виконання потрібних функцій із заданим рівнем характеристик [1]. Користувачі можуть гарантовано довіряти послугам ІС за наявності функціональної стійкості системи, що характеризує здатність системи зберігати (автоматично відновлювати) виконання повного або прийнятного набору функцій в умовах деструктивних впливів на ІС. Функціональна стійкість ІС передбачає наявність у системи певного рівня надійності, відмовостійкості, адаптивності, живучості. Зазвичай функціональна стійкість ІС забезпечується введенням певної надмірності; провадженням системи вбудованого контролю; формуванням контуру захисту від негативних впливів зовнішнього середовища; використанням компонентів із підвищеним рівнем захищеності і надійності. Та на жаль, додаткова надмірність веде до погіршення техніко-економічних характеристик ІС. Системи контролю відстежують заданий ряд параметрів, але не завжди забезпечують адекватну реакцію на нештатну ситуацію, до того ж не зменшується ймовірність виникнення таких ситуацій. Контур захисту мінімізує вплив зовнішніх факторів, але повністю його не виключає. Вибір елементної бази з підвищеним рівнем захищеності й надійності підвищує відмовостійкість ІС, та не забезпечує функціональної стійкості, коли відмова вже сталася.

Один із визнаних успішних шляхів підвищення функціональної стійкості ІС спирається на принцип *багатоверсійності (*або *диверсності)*. Цей принцип передбачає програмно-апаратну та/або функціональну надмірність та різноманіття. Диверсність застосовується для компенсації ризиків у системах, вимогливих до безпеки, насамперед, у системах спеціального призначення.

Згідно з принципом багатоверсійності функціональна стійкість ІС забезпечується використанням різноманітних продуктових (апаратно-програмних) і процесорних засобів для реалізації ідентичних функцій системи. Принцип багатоверсійності спирається на властивість адаптивності, що базується на введенні надмірності (часової, апаратної та програмної) та засобів контролю, діагностування та реконфігурації. Актуальним є застосування багатоверсійності для підвищення функціональної стійкості ІС, інтегрованих у критичні інфраструктури, порушення функціонування яких веде до аварій, катастроф та екологічних лих. Багатоверсійність вже зараз реалізується в ІС критичних об'єктів (в авіації, космонавтиці, хімічній

промисловості, залізничному транспорті, АЕС) та регламентується національними та міжнародними стандартами, хоча ще потребують вирішення питання гармонізації вимог міжнародних та національних стандартів щодо використання диверсності в різних застосунках; типів версійної надмірності та моделі багатоверсійного програмного забезпечення та життєвого циклу систем; диверсність систем числення; метрики диверсності та методи оцінки багатоверсійних систем; аналіз досвіду розробки та застосування багатоверсійного програмного забезпечення; оптимальне резервування при різнотипних компонентах [2].

Багатоверсійність сьогодні можна вважати концептуальним підходом до комплексного вирішення проблеми виявлення та парирування відмов, викликаних фізичними дефектами апаратних засобів, дефектами проектування програмних засобів і зовнішніми впливами інформаційного та іншого характеру. Та в рамах такої галузі науки і практики, як функціональна стійкість ІС, на поточний момент недостатньо опрацьовані питання:

- практичної оцінки надійності програмного забезпечення ІС;
- прогнозування, раннього виявлення та попередження, протидії руйнівним інформаційним впливам зовнішнього середовища;
- розробки механізмів підвищення живучості ІС.

Дослідження, спрямовані на попередження атак на критичні інфраструктури з урахуванням досвіду попередніх атак, які призвели до внесення структурних, архітектурних та інших змін в критичні інфраструктури, до певної функціональної еволюції цих інфраструктур як системних утворень, виокремлюються сьогодні у контексті формування поняття резильєнтності критичних інфраструктур. Поняття резильєнтності змістовно визначається так само, як живучість критичних інфраструктур з точки зору кібербезпеки [3]. На наш погляд, введення до наукового обігу нового поняття потребує не лише певного узгодження з існуючою термінологічною системою, а й слугувати поглибленню теоретичних досліджень і розв’язанню актуальних практичних задач.

1 Oleksandr Dodonov, Olena Gorbachyk, Maryna Kuznietsova. Automated Organizational Management Systems of Critical Infrastructure: Security and Functional Stability. CEUR Workshop Proceedings 2021, 3241, pp.1-12. http://ceur-ws.org/Vol-3241/paper1.pdf

2 Харченко В.С., Яковлев С.В., Горбачик О.С. та ін. Забезпечення функціональної безпеки критичних інформаційно-керуючих систем. Харків: Константа, 2019. 272 с.

3 Лисенко С.М., Харченко В.С., Бобровнікова К.Ю., Щука В.Р. Резильєнтність комп’ютерних систем в умовах кіберзагроз: таксономія та антологія // Радіоелектронні і комп’ютерні системи, 2020. №1(93). С.17-28. doi: 10.32620/reks.2020.1.02.

І.В. Блінов

АСПЕКТИ ВПРОВАДЖЕННЯ СУЧАСНИХ ЄВРОПЕЙСЬКИХ ТА МІЖНАРОДНИХ СТАНДАРТІВ В СФЕРІ SMART GRID ЗАДЛЯ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ УКРАЇНИ

Сьогодні важливою частиною політики Європейського Союзу (ЄС) в галузі електроенергетики є комплекс заходів, що об'єднаний терміном «енергетичний перехід» (англ. Energy Transition) [1]. Важливою складовою такого переходу є цифрова трансформація електроенергетичної галузі – зміна звичних бізнес-моделей завдяки цифровим технологіям та забезпечення нових можливостей щодо отримання додаткової вартості у нових чи існуючих сегментах ринку електричної енергії чи надання послуг (надання нових можливостей для отримання доходу та створення додаткової вартості). Узагальнено цифрова трансформація може бути визначена як нове використання цифрових технологій для прискорення бізнес-стратегії.

Європейською технологічною та інноваційною платформою інтелектуальних мереж для енергетичного переходу (European Technology and Innovation Platform for Smart Networks for Energy Transition, ETIP SNET)) у 2018 р. був розроблений базовий документ ETIP-SNET Vision 2050 задля здійснення енергетичного переходу в ЄС [2]. Планується, що у 2050 році інтегровані енергетичні системи складатимуться з чотирьох взаємопов'язаних і взаємозалежних рівнів, які стимулюватимуть економічне зростання та глобальну конкурентоспроможність для Європи:

1) ринковий рівень – дозволяє обмінюватися інформацією між учасниками ринку;

2) комунікаційний рівень – підтримує вертикальну та горизонтальну інтеграцію енергетичних систем та обмін інформацією з ринком;

3) рівень фізичної системи – складається з автоматизованих енергетичних інфраструктур, розроблених для задоволення потреб споживачів;

4) рівень цифрової інфраструктури – підтримує мережеві операції для управління інтегрованими енергетичними системами з більш високим рівнем автоматизації, бачення та підзвітності.

Цифрова трансформація [3] передбачає побудову «розумної» електроенергетичної системи, що орієнтована на вирішення проблем оптимізації загальної ефективності та балансу низки взаємопов'язаних енергетичних технологій та процесів як електричних, так і неелектричних.

Для забезпечення цифрової трансформації Міністерство енергетики України розробило «Концепцію впровадження "розумних мереж" в Україні до 2035 року» [4], в якій розкрито поняття «розумних мереж», визначено загальні напрямки впровадження і використання технологій «розумних мереж» в енергетичному секторі України, встановлено пріоритети і основні

механізми реалізації, встановлено етапи і коло ключових учасників впровадження технологій «розумних мереж».

У цій Концепції зазначено, що платформа просування «розумних мереж» в Україні спирається на готовий набір технологій і заходів, визначених у європейських та міжнародних стандартах, які визначають технологічні рішення реалізації для кожного компонента енергетичного сектора, а також готовий набір телекомунікаційних та інформаційних протоколів, що сприяють реалізації цих технологій.

Існуючий курс «Концепції впровадження «розумних мереж» в Україні до 2035 року» направлений на активний розвиток систем Smart Grid [5, 6] в енергетичній системі України відповідає пріоритетним напрямкам розвитку енергетики в ЄС, а також задачам, які потребують розв'язку при синхронній роботі ОЕС України та ENTSO-E.

Згідно Концепції в Україні процес розвитку необхідної нормативно-технічної бази має спиратися на такі основні принципи як: застосування існуючого набору технологій і заходів, визначених Європейським комітетом з електротехнічної стандартизації (CENELEC) для кожного компонента енергетичного сектора; застосування наявного пакету міжнародних стандартів, включаючи телекомунікаційні та інформаційні протоколи, розроблені IEC, що сприяють реалізації технологій "розумних" мереж та ринків електричної енергії.

Забезпечення процесів цифрової трансформації в електроенергетичній галузі України, в свою чергу, потребує прийняття пріоритетних сучасних європейських та міжнародних стандартів в сфері впровадження технологій Smart Grid. До основних функціональних систем SmartGrid, які є найбільш актуальними для розвитку електроенергетичної системи України та потребують впровадження відовідних стантартів згідно IEC TR 63097:2017 відносяться наступні [7]:

- система управління генерацією (Generation Management System);
- гнучкі системи передачі змінного струму (FACTS for grids);
- система енергетичного менеджменту (Energy Management system);
- система запобігання системним аваріям в енергосистемі (Black out Prevention System);
- вдосконалена система управління розподілом (Advanced Distribution Management System);
- система автоматизації розподілу (Distribution Automation System);
- система автоматизації роботи підстанцій (Substation Automation System);
- система управління розосередженими енергетичними ресурсами (Distributed Energy Resources Operation System);
- удосконалена інфраструктура обліку енергії (Advanced Metering Infrastructure);
- система управління ринками (Market places system);
- реагування на попит / управління навантаженням (Demand Response/Load Management);

- система зберігання електричної енергії (Electrical Energy Storage System).

Впровадження стандартів із зазначених напрямків має враховувати нові міжнародні стандарти відповідної сфери застосування, що з'явилися після 2017 р., через що не були включені до стандарту IEC TR 63097:2017.

Все це обумовлює актуальність та важливість завдання, що сьогодні стоїть в електроенергетичній сфері України, щодо реалізації заходів з розроблення стратегії та створення дорожньої карти для прийняття сучасних європейських та міжнародних стандартів в сфері електроенергетики та електротехніки, важливою складовою якого є визначення пріоритетних стандартів, які потребують впровадження в Україні та є базовими для забезпечення впровадження технологій Smart Grid [8, 9]. Це дозволить прискорити процеси стандартизації в електроенергетиці та електротехніці України у відповідності з сучасними світовими тенденціями та забезпечить виконання зобов'язань України в рамках співпраці з Європейським Союзом.

1 Кириленко О.В. Заходи та засоби перетворення енергетики України на інтелектуальну екологчно безпечну системи. 2022. Вісн. НАН України. № 3. С. 18-23. doi: https://doi.org/10.15407/visn2022.03.018

2 ETIP SNET VISION 2050. Integrating Smart Networks for the Energy Transition: Serving Society and Protecting the Environment. European Commission. 2018. P. 52.

3 A Brief Roadmap for Digital Transformation: Leveraging Business Architecture to Achieve Superb Results. – https://www2.deloitte.com/rs/en/pages/strategy-operations/articles/brief-roadmap-for-digital-transformation-leveraging-business-architecture-to-achieve-superb-results.html

4 Про схвалення Концепції впровадження "розумних мереж" в Україні до 2035 року. Розпорядження КМУ № 908-рвід 14 жовтня 2022 р

5 Кириленко О.В., Блінов І.В., Зайцев Є.О. Палачов С.О., Васильченко В.І. Впровадження міжнародних та європейських стандартів для розвитку ОЕС України згідно концепції Smart Grid. Праці Інституту електродинаміки Національної академії наук України. 2022. № 63. С. 5-12. doi: https://doi.org/10.15407/publishing2022.63.005

6 Танкевич С.Є., Блінов І.В., Кириленко В.В. Україна та світ: нормативне забезпечення інтелектуальних електроенергетичних систем за концепцією Smart Grid. Стандартизація, сертифікація, якість. 2014. №4 (89). С. 38–44.

7 IEC/TR 63097:2017 Smart grid standardization roadmap. 2017. 315 p.

8 Кириленко О.В., Блінов І.В., Танкевич С.Є. Smart Grid та організація інформаційного обміну в електроенергетичних системах. Технічна електродинаміка. 2012. № 3. С. 47 – 48.

9 Блінов І.В., Парус Є.В., Шкарупило В.В. Структура та моделі інформаційної взаємодії учасників ринку електричної енергії. Вінниця: ГО «Європейська наукова платформа», 2021, 114 с. DOI: https://doi.org/10.36074/stmivyree-monograph.2021

В.В. Шкарупило, А.А. Пацьора, В.В. Душеба

ЩОДО АСПЕКТІВ ДОСЯГНЕННЯ РЕЗИЛІЄНТНОСТІ ЗА АДАПТАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ДО ІТЕРАЦІЇ WEB 3.0

У наш час все більшого поширення набуває концепція Web 3.0 – концепція в основі подальшої ітерації розвитку глобальної мережі, що будується, у тому числі, на засадах принципу децентралізації, зокрема із залученням технології Blockchain [1]. Разом із цим, сучасні інформаційні засоби, а також комп'ютерні системи, побудовані на їх основі, вже зарекомендували себе у якості дієвих інструментів уможливлення результативного освітнього процесу, зокрема орієнтованого на підготовку фахівців у галузі енергетики, і реалізованого в умовах поточних реалій: ризиків, зумовлених зовнішньою агресією; обмежень, спричинених введенням воєнного стану тощо. Зазначене досягається, зокрема, шляхом перенесення освітніх порталів у хмарне середовище. Особливої вагомості цей аспект набув, у тому числі, у зв'язку із систематичними атаками окупаційної сторони на енергетичний сектор України [2]. Зниження небажаних наслідків, обумовлених такими діями, досягається, зокрема, шляхом розвитку механізмів забезпечення резилієнтності (resilience) в енергетичному секторі [3]. При цьому постають виклики з позицій кібербезпеки і кіберзахисту як названих систем безпосередньо, так і каналів зв'язку між системами і користувачами зокрема.

Варто зазначити, що в актуальних публікаціях на окреслену тематику властивість резилієнтності розглядається з точки зору здатності досліджуваної системи як витримувати небажаний вплив зовнішніх чинників, зберігаючи функціонування, так і відновлюватися – якщо функціонування системи було унеможливлено [4 – 6]. Більше того, доцільним вбачається охоплення поняття резилієнтності саме у контексті парадигми керування інформаційною системою – у розрізі супроводження останньої упродовж усього життєвого циклу [4]. І дійсно, з урахуванням ad-hoc-природи сценаріїв, що мають місце за актуалізації освітнього процесу, у тому числі за адаптації останнього до засад Web 3.0, доцільним вбачається розроблення методик, прийомів, підходів, покликаних надавати дієві механізми реалізації резилієнтних ad-hoc-сценаріїв, що мають місце у сучасному освітньому середовищі, що поступово розвивається у напрямі Web 3.0. Це можливо, зокрема, як шляхом диверсифікації застосовуваних освітніх, інформаційних технологій, програмно-апаратних засобів тощо, так і шляхом комбінування останніх.

Таким чином, у розрізі актуальних подій в Україні, концепція резилієнтності набуває особливої ваги. При цьому у межах праці зроблено наголос на важливості охоплення і опрацювання властивості резилієнтності інформаційних систем, залучених у якості засобів, що уможливлюють реалізацію сучасного освітнього процесу, зокрема у контексті адаптації

останнього до ітерації Web 3.0. Більше того, зазначено, що запорукою названого є резилієнтність енергетичної інфраструктури України.

1 Monrat, A.A., Schelén, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access*, 7, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094

2 Nikolaieva, I., & Zwijnenburg, W. (2022). Risks and impacts from attacks on energy infrastructure in Ukraine. PAX report. Dec. 2022. https://paxforpeace.nl/media/download/PAX_Ukraine_energy_infrastructure_FIN.pdf

3 Jasinas, J., Lund, P.D., & Mikkola, J. (2021). Energy system resilience – A review. *Renewable and Sustainable Energy Reviews*, 150. https://doi.org/10.1016/j.rser.2021.111476

4 Linkov, I., Bridges, T., Creutzig, F. et al. (2014). Changing the resilience paradigm. *Nature Climate Change*, 4, 407–409. https://doi.org/10.1038/nclimate2227

5 Ganin, A.A., Kitsak, M., Marchese, D., Keisler, J.M., Seager, T., & Linkov, I. (2017). Resilience and efficiency in transportation networks. *Science Advances*, 3(12). https://doi.org/10.1126%2Fsciadv.1701079

6 Linkov, I., & Trump, B.D. (2019). *The Science and Practice of Resilience*. Springer. ISBN 978-3-030-04563-0. https://doi.org/10.1007/978-3-030-04565-4

А.О. Запорожець

РОЛЬ МОНІТОРИНГУ В УПРАВЛІННІ ЯКІСТЮ ПОВІТРЯ В ОКОЛІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Моніторинг навколишнього середовища проводиться для контролю за його станом, забезпечення державних органів, юридичних та фізичних осіб достовірною та оперативною інформацією, необхідною для своєчасного реагування на зміни навколишнього середовища, та раціонального користування природними ресурсами [1]. При цьому особливої уваги на даний час набуває моніторинг в околі об'єктів критичної інфраструктури.

Моніторингом забруднення атмосферного повітря є система комплексних довгострокових спостережень, що виконуються за чітко встановленою програмою, на протязі тривалого часу за станом повітря, його забрудненням, природними явищами, що в ньому виникають, а також оцінювання та прогноз параметрів, що характеризують його стан. При цьому моніторинг забруднення атмосферного повітря є складовою частиною державної системи моніторингу навколишнього середовища.

На рис. 1 наведено класифікацію параметрів, що характеризують стан атмосферного повітря.

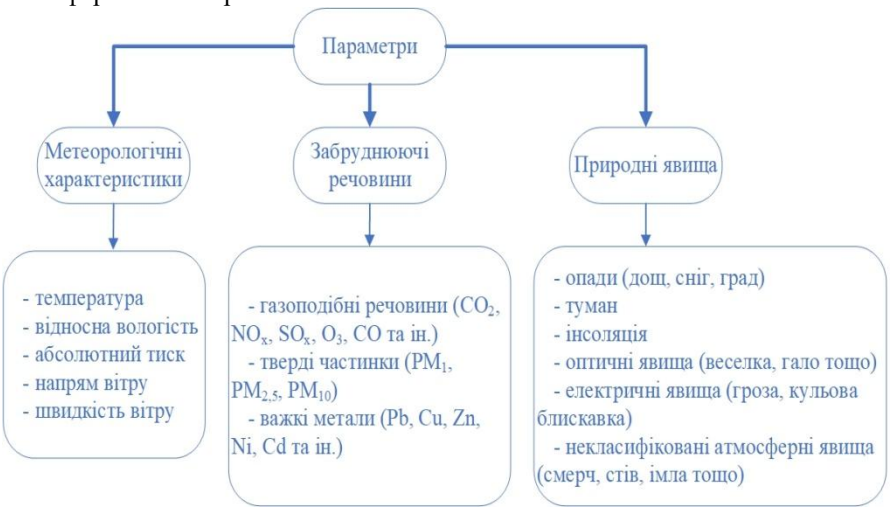


Рисунок 1 – Класифікація параметрів стану атмосферного повітря

Головна задача моніторингу атмосферного повітря полягає не у накопиченні даних, отриманих з постів спостереження, а у отриманні інформації, необхідної для прийняття рішень в сфері управління якістю атмосферного повітря та покращення його санітарного стану. Моніторинг в цьому процесі відіграє роль наукової бази для розробки стратегій та прийняття рішень, постановці завдань, оцінюванні досягнень заданих цілей,

плануванні заходів по реалізації законодавчих актів та контролю за їх виконанням (рис. 2).

Рисунок 2 – Моніторинг в управлінні якістю атмосферного повітря

Однак, звичайно, моніторинг не може бути єдиним засобом для комплексного управління якістю атмосферного повітря. В багатьох великих та малих містах, на території об'єктів критичної інфраструктури та інших зонах часто є недостатнім і недоцільним використання тільки прямих вимірювань параметрів стану атмосферного повітря. Тому разом з моніторингом потрібно використовувати різні методи оцінки стану атмосферного повітря, включаючи моделювання розповсюдження полютантів, метеорологічних характеристик та атмосферних явищ, картування, інтерполяцію та ін.

Потрібно зважати на те, що жодна система моніторингу, якою б за матеріально-технічною базою вона не була, не може отримати всі необхідні просторово-часові характеристики параметрів стану атмосферного повітря. При цьому те саме твердження відноситься і до окремого використання тільки систем моделювання (наприклад, Copernicus), адже моделі мають бути верифіковані на основі даних прямих вимірювань в процесі моніторингу. Таким чином, такий дуалістичний підхід дозволить максимально ефективно використати наявні технічні ресурси та максимізувати ефект від впровадження комплексної системи моніторингу забруднення атмосферного повітря.

Варто відмітити, що моніторинг забруднення атмосферного повітря – це систематичний, ресурсоємний і тривалий процес, який має здійснюватися державними органами. Проте на даний час велика кількість аналітиків та

експертів відзначають, що в Україні відсутня будь-яка державна програма з фінансування сучасної мережі моніторингу.

В Директиві 2008/50/ЄС відзначено, що вона визнає доцільність використання в державах, що її імплементували, різних методів моніторингу, моделювання та об'єктивного аналізу при оцінюванні стану забруднення атмосферного повітря. Вибір будь-якого методу залежить від існуючої матеріально-технічної бази та поточного стану атмосферного повітря на території, де проводиться моніторинг.

Незважаючи на те, що Україна ратифікувала цю директиву, тільки Постановою Кабінету міністрів України від 14 серпня 2019 р. №827 про «Деякі питання здійснення державного моніторингу в галузі охорони атмосферного повітря» було створено нормативно-правову базу, що узгоджувала існуюче законодавство з ратифікованою Директивою. Зокрема важливо відмітити наступні нововведення для вітчизняного моніторингу:

1. встановлені верхні та нижні межі оцінки, цільові та граничні значення для основних полютантів;

2. введення моніторингу забруднення мілкодисперсним пилом (твердими частинками) $PM_{2,5}$, PM_{10} та озоном O_3;

3. методом підтвердження прийнято ряд європейських стандартів для вимірювання концентрації різних полютантів в повітрі;

4. встановлено можливість проведення індикативних вимірювань для великої кількості полютантів, зокрема $PM_{2,5}$, PM_{10}, SO_2, NO_2, NO, CO, O_3, важких металів (Ar, Cd, Ni, тощо), та ін.;

5. введено цілі щодо якості даних для оцінки якості атмосферного повітря для великої кількості полютантів.

При цьому у вітчизняній мережі моніторингу забруднення атмосферного повітря залишається ряд невирішених проблем:

1. відсутність систематичного фінансування;

2. відсутністю комунікаційної стратегії;

3. відсутність стратегії розвитку мережі моніторингу.

1. Запорожець А. О. Науково-практичні засади створення засобів та методів контролю забруднення повітря об'єктами енергетики : дис. докт. техн. наук : 05.11.13 / Запорожець Артур Олександрович – Київ, 2022. – 539 с.
2. Деякі питання здійснення державного моніторингу в галузі охорони атмосферного повітря [Електронний ресурс] // Постанова Кабінету міністрів України від 14 серпня 2019 р. №827. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/827-2019-%D0%BF#Text.

С.О. Євдокимов, В.П. Таранущенко

ВИКОРИСТАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ ПІД ЧАС ВОЄННОГО СТАНУ

Для спеціалістів різноманітного профілю актуальною є підготовка даного питання. Зокрема, проблема виявлення факторів ймовірної небезпеки ДТП є однією з найскладніших завдань у сфері інформаційних технологій через велику різноманітність викривлень, таких як різний вираз навколишнього середовища, умови зйомки та ін. Для вирішення даного завдання ефективно використовувати нейронні мережі в зв'язку з тим, що вони слабо чутливі і мають високу швидкість розпізнавання.

В рамках даної роботи було проведено дослідження впливу різних факторів на кількість адміністративних та кримінальних правопорушень у сфері дорожнього руху. Було проаналізовано статистичні дані правопорушень та дорожньо-транспортних пригод в Україні та деяких держав Європейського союзу. Відповідно до цього виділено наступні фактори:

- характеристики видимості дороги (ухили, повороти);
- погодні умови, час доби та сезонність;
- стан дорожньої обстановки, призначення дороги;
- додаткові швидкісні обмеження на цій ділянці;
- відстань від населеного пункту;
- інтенсивність руху;
- наявність розмітки, ширина та кількість смуг.

Завдання, які вирішуються для досягнення поставленої мети:

1. Вивчення існуючих програмних засобів основаних на нейронній мережі щодо попередження інцидентів ДТП.
2. Вибір пристроїв апаратного та програмного забезпечення.
3. Розробка алгоритмів для управління роботою об'єктів.
4. Реалізація розроблених алгоритмів на обраному ПЗ.

Для розробки даного проекту необхідно дотримуватися структури ШНМ для системи автоматизації. Дана архітектура представляє послідовність шарів згортки, які спершу зменшують просторову роздільну здатність картинки, а потім збільшують його, попередньо об'єднавши з даними і пропустивши через інші шари згортки.

Суть методу, запропонованого у роботі, метод призначений для управління в аварійній ситуації ТЗ. полягає в тому, що після накопичення за кілька тактів часу інформації про дорожню обстановку, що надходить від різних джерел, та формування відповідності, здійснюється класифікація ситуації – віднесення її до відповідної категорії.

Рисунок 1 – Фрагмент в програмному середовищі Jupyter Notebook. Генерація наборів станів

Для перевірки працездатності методу було здійснено моделювання ситуації обгону на двополосній дорозі, де обгін проводиться з виїздом на смугу зустрічного руху. При моделюванні з використанням нейромережі *TensorFlow* використовувалися два шари *tf.keras.layers. Dense*. Навчання проводилося на 5 етапах (Рисунок 2).

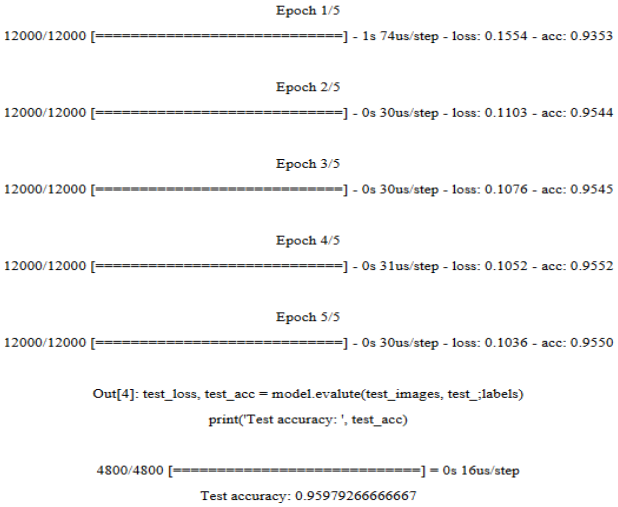


Рисунок 2 – Моделювання на виявлення аварійно-небезпечної ситуації

Точність розпізнавання аварійної ситуації при обгоні склала приблизно 0,92. Оцінка швидкодії розв'язання задачі, що була представлена у роботі, не проводилася, так як на даному етапі така оцінка є тимчасової. Тому, використання згорткової нейронної мережі для обробки інформації про дорожню обстановку дозволяє виявляти ДТП, а інтеграція такого алгоритму у системах керування автомобілем може запобігати ДТП.

Висновки та рекомендації роботи можуть знайти конкретну реалізацію в діяльності державних установ Головного управління Національної поліції України, Департаменту Патрульної поліції НПУ України, а також в приватних організаціях, в частині пропозицій щодо реалізації системи управління діяльністю підприємств у контексті забезпечення його конкурентоспроможності.

1. Cremer M., Ludwig J. A fast simulation model for traffic flow on the basis of Boolean operations // Mathematics and Computers in Simulation. 1986. V. 28. N 4. P. 297–303. doi: 10.1016/0378-4754(86)90051-0
2. Alvarez I., Poznyak A., Malo A. Urban traffic control problem via a game theory application // Proc. 46th IEEE Conference on Decision and Control (CDC 2007). 2007. P. 2957–2961. doi: 10.1109/CDC.2007.4434820
3. Dai J., Li Y., He K., Sun J. R-FCN: Object detection via region-based fully convolutional networks // Proc. 30 th Annual Conference on Neural Information Processing Systems (NIPS 2016). P. 379–387
4. Serhii Yevdokymov, Volodymyr Taranushchenko. Prospects of using a conversion neural network to prevent traffic accidents in a popular point. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 76): матеріали Міжнародної наукової інтернет- конференції, (м. Тернопіль, Україна – м. Переворськ, Польща, 3-4 квітня 2023 р.) / [редкол.: О. Патряк та ін.]; ГО “Наукова спільнота”; WSSG w Przeworsku. – Тернопіль: ФО-П Шпак В.Б. – С. 10-11
5. Євдокимов С.О. Побудова штучних нейронних мереж на основі теорії мотивації соціального вивчення та психофізичних реакцій людини сформованих з дитинства. Розвиток освіти і науки як стратегія формування культури майбутнього. Гуманітарний корпус. Випуск 50: збірник ІІ-ої Міжнародної науково-практичної конференції (7 квітня 2023 року, м. Київ). –Київ: Національний педагогічний університету імені М.П. Драгоманова, 2023. С.58-61 https://nnifop.udu.edu.ua/index.php/uk/nauka/konferentsii/258-ii-mizhnarodna-naukova-konferentsiia-rozvytok-osvity-i-nauky-yak-stratehiya-formuvannya-kultury-maybutnoho-07042023-ua-pl

А.В. Давидюк, Ю.Є. Хохлачова, В.Ю. Зубок

КОНЦЕПЦІЯ ЦЕНТРУ КІБЕРСТІЙКОСТІ ДЛЯ УКРАЇНИ

З урахуванням постійних динамічних змін у законодавстві України в галузі інформаційної та кібербезпеки та впровадження нових механізмів та технічних рішень для забезпечення кіберзахисту інформаційно-комунікаційних систем, виникає необхідність розробки моделей стійкості систем кіберзахисту державних органів та об'єктів критичної інфраструктури. Під стійкістю в кіберпросторі розуміється можливість систем кіберзахисту до швидкої інтеграції в нові ІКС та адаптації до змін в існуючих, шляхом визначення оптимальних шляхів та ресурсів для цих процесів. З огляду на зазначене доцільним є створення Центр кіберстійкості для України у формі Центру компетенцій (далі - Центр). У світи вже давно існує практика створення та інтеграції центрів кіберстійкості, найбільш потужними і відомими є Cyber Resilience Centre for Greater Manchester (CRCGM) [1], Cyber Resilience Centre for the South West (CRC-SW) [2], Scottish Business Resilience Centre (SBRC) [3], Cyber Wales [4], Australian Cyber Collaboration Centre (A3C) [5], The Cyber Resilience Centre for London [6], що підтверджує актуальність даної ідеї.

Концепція Центру полягає у спільній ініціативі, спрямованій на підвищення рівня кібербезпеки та стійкості організацій різної форми власності. Центр працюватиме на державному рівні і служитиме надійним центром експертних знань, ресурсів і підтримки з кібербезпеки.

Основні цілі Центру кіберстійкості включають:

Сприяти обізнаності і освіті. Центр повинен мати на меті підвищити обізнаність про загрози кібербезпеці та найкращі практики серед державних та приватних організацій і громад, створювати і надавати освітні ресурси, навчальні програми та навчальні матеріали, щоб допомогти розвинути міцну культуру кібербезпеки.

Участь у реагуванні на інциденти та підготовці кібероперацій для кібероборони. Центр повинен мати ресурси для реагування на інциденти, щоб допомогти організаціям ефективно реагувати на кіберінциденти та сприяти заходам з кібероборони. Це може включати надання технічної допомоги під час кібератак або в процесах відновлення.

Здійснювати заходи з розвідки загроз та обміну інформацією: Центр збиратиме, аналізуватиме і поширюватиме інформацію про загрози своїм партнерам і зацікавленим сторонам. Обмінюючись інформацією про нові загрози, уразливості та тенденції атак, Центр допомагатиме організаціям бути в курсі та краще захищатися від кіберзагроз.

Забезпечувати надання послуг та консультацій з кібербезпеки, щоб допомогти організаціям оцінити та покращити стан кібербезпеки. Це може включати проведення оцінок безпеки, сканування вразливостей, тестування

на проникнення, стрестестування та надання рекомендацій щодо впровадження заходів безпеки.

Сприяти партнерству та співпраці, Центр забезпечуватиме співпрацю між різними зацікавленими сторонами, включаючи правоохоронні органи, державні установи, організації приватного сектору та наукові кола. Об'єднуючи експертизу з різних галузей економіки, Центр сприятиме обміну інформацією, спільним ініціативам і розвитку екосистем кібербезпеки.

Створення Центру доцільно здійснювати на базі наукових установ, що мають потенціал в сфері кібербезпеки. Дослідження робіт [6-9], присвячених побудові Центрів кіберстійкості та впровадження процесів кіберстійкості допомогли виділити пріоритетні завдання Центру.

Основними завданнями Центру будуть:

Експертиза кіберстійкості існуючої нормативної бази в сфері кібербезпеки;

Експертиза кіберстійкості відомчих нормативних документів з кібербезпеки;

Експертиза кіберстійкості політик безпеки організацій.

Розробка методик стрестестування для процесів кібербезпеки.

Надання пропозицій в частині кіберстійкості до нормативних документів з кібербезпеки.

Проведення оцінки ризиків кіберстійкості в рамках незалежних аудитів кібербезпеки.

Оцінювання планів забезпечення неперервності бізнесу.

Проведення навчань з кіберстійкості для суб'єктів забезпечення кібербезпеки.

Проведення конференцій з проблем кіберстійкості.

Здійснення аналітичних оглядів проблем кіберстійкості в Україні та світі.

Залучення міжнародного потенціалу в сфері кіберстійкості.

Участь у проєктуванні нових систем кіберзахисту в частині, що стосується кіберстійкості.

Проведення науково-дослідних робіт в сфері кіберстійкості.

Надання консультацій при плануванні кібероперацій.

Надання консультацій щодо впровадження процесів кіберстійкості.

Центр під час війни може сприяти у реагуванні на кіберінциденти, здійснювати обмін інформацією, формувати міжнародні відносини в сфері кіберстійкості шляхом обміну досвідом та знаннями, здійснювати підтримку процесів кібербезпеки в країні.

Після війни пріоритетними завданнями центру мають стати післявоєнне відновлення систем і побудова нових систем кібербезпеки, відновлення мереж комунікацій, критичної інфраструктури, надавати експертні знання та ресурси для покращення практики кібербезпеки та кіберстійкості у післявоєнний період. Центр може сприяти розбудові спроможності, зокрема може відігравати важливу роль в ініціативах з забезпечення навчання та передачі знань для підвищення навичок кіберстійкості українських

організацій, державних установ та громадян. Це допоможе підвищити загальну кіберстійкість країни. Центр кіберстійкості може співпрацювати з українською владою у розробці державної політики в сфері кіберстійкості, нормативних актів і фреймворків з кібербезпеки, спрямованих на вирішення конкретних проблем, з якими зустрічаються під час і після війни. Ці політики можуть допомогти створити стійку кібер-екосистему в країні.

Центр кіберстійкості може допомогти Україні посилити захист кібербезпеки, розробити проактивні стратегії та покращити можливості реагування на інциденти, щоб зменшити вплив кібератак. Критична інфраструктура України, включаючи енергетичні, транспортні та комунікаційні системи, залишається вразливою до кіберзагроз. Центр кіберстійкості може тісно співпрацювати з цими секторами, щоб виявити вразливі місця, розробити стратегії управління ризиками та впровадити надійні заходи кібербезпеки для захисту критичної інфраструктури від потенційних збоїв під час конфлікту чи в умовах підвищених ризиків. Центр сприятиме міжнародній співпраці та обміну інформацією для протидії кібератакам з боку не дружніх держав. Окремо варто виділити економічний вплив появи Центру в Україні - надійна кібербезпека має вирішальне значення для економічного зростання та залучення іноземних інвестицій. Створивши центр кіберстійкості, Україна може продемонструвати свою підвищену зацікавленість у кібербезпеці, що може вселити довіру серед бізнесу, інвесторів та міжнародних партнерів. Це, у свою чергу, може сприяти економічному розвитку та стійкості країни. Центр може відігравати ключову роль у нарощуванні потенціалу з кіберстійкості, надаючи навчальні програми, семінари та освітні ініціативи. Удосконалюючи навички та знання з кіберстійкості в різних секторах, Центр може надати можливість окремим особам, організаціям і державним установам краще протистояти кіберзагрозам.

Загалом, центр кіберстійкості може слугувати життєво важливим активом для України у зміцненні її кібербезпеки, захисті критичної інфраструктури, сприянні економічному розвитку, розбудові потенціалу та сприянні співпраці. Інвестуючи в кіберстійкість, Україна може краще захистити свою національну безпеку, забезпечити безперервність основних послуг і пом’якшити ризики, пов’язані з кіберзагрозами під час і після конфлікту.

1 *North west cyber resilience centre*. (б. д.). NWCRC. https://www.nwcrc.co.uk/

2 *The Cyber Resilience Centre for the South West*. (б. д.). SWCRC. https://www.swcrc.co.uk/

3 *Home - Cyber and Fraud Centre - Scotland*. (б. д.). Cyber and Fraud Centre - Scotland. https://cyberfraudcentre.com/

4 *Cyber Wales | A Flourishing Cyber Ecosystem*. (б. д.). Cyber Wales | A Flourishing Cyber Ecosystem. https://www.cyberwales.net/

5 *Home - Cyber Security Resilience Centre - London CRC*. (б. д.). Home - Cyber Security Resilience Centre - London CRC. https://www.londoncrc.co.uk/

6 Blokdyk, G. (2020, 16 квітня). *Cyber resilience A complete guide - 2020 edition, автор: Gerardus blokdyk – электронная книга | scribd*. Scribd. https://ru.scribd.com/book/456779401/Cyber-Resilience-A-Complete-Guide-2020-Edition

7 *Boosting your organisation's cyber resilience - joint publication*. (б. д.). ENISA. https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

8 *The Cyber Resilience Centre for the South West*. (б. д.). SWCRC. https://www.swcrc.co.uk/

9 *Cyber resilience: Playbook for public-private collaboration | digital watch observatory*. (б. д.). Digital Watch Observatory. https://dig.watch/resource/cyber-resilience-playbook-public-private-collaboration

В.В. Філатов, О.В. Попко

РЕЗИЛЬЄНТНІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ НА РИНКУ ЕЛЕКТРОТЕХНІЧНОГО ОБЛАДНАННЯ

Резильєнтність критичної інфраструктури відноситься до її здатності відновлюватися, адаптовуватися і функціонувати ефективно в умовах різних видів стресу, таких як природні катастрофи, техногенні аварії, кібератаки, терористичні акти тощо [1]. Це важливий аспект безпеки та стабільності суспільства і економіки.

Основні принципи резильєнтності критичної інфраструктури включають [2]:

1. Розподілені системи. Інфраструктурні системи повинні бути розподілені географічно, щоб уникнути їх повного збою у разі виникнення надзвичайних ситуацій, аварій чи катастроф в одній області та запобігти їх поширенню в інших областях.

2. Резервування. Резильєнтна інфраструктура повинна мати певні системи для резервування необхідних ресурсів. Це може означати наявність альтернативних джерел енергії, запасних комунікаційних мереж, дублювання критичних компонентів та інших заходів, що забезпечують продовження роботи в умовах непередбачуваних (форс-мажорних) обставин.

3. Адаптивність і гнучкість. Резильєнтна інфраструктура повинна бути гнучкою і адаптивною до зміни умов зовнішнього середовища, а також мати налагоджений механізм швидкого реагування на зовнішні небезпеки, включаючи: виявлення проблеми, автоматичне переключення на резервні системи живлення, можливість швидкого відновлення діючих компонентів.

4. Керованість і координація. Ефективне управління і координація між різними секторами інфраструктури, органами влади, операторами інфраструктури та іншими зацікавленими сторонами є ключовими аспектами резильєнтності критичної інфраструктури. Співробітництво і обмін інформацією між всіма зацікавленими сторонами дозволяють вчасно виявляти загрози, адекватно реагувати на них і координувати відновлення після настання непередбачуваної події, що, своєю чергою, потребує створення міжсекторальних комітетів або організацій, спільні тренування і планування для виявлення й реагування на небезпеки, обмін інформацією про критичну інфраструктуру й потенційні загрози, а також розробку спільних протоколів дій у випадку аварій або кризових ситуацій.

Ефективна керованість і координація передбачають наявність плану дій у випадку настання надзвичайної ситуації, який визначатиме ролі та відповідальність різних структурних підрозділів та органів влади. Такі плани повинні періодично оновлюватись і випробовуватись на практиці, щоб завчасно переконатися в їхній ефективності.

Резильєнтність критичної інфраструктури вимагає комплексного підходу, який передбачає технічні, організаційні та стратегічні заходи. Основні ключові компоненти цього підходу включають [2]:

1. Оцінку ризиків. Проведення систематичної оцінки можливих ризиків допомагає ідентифікувати потенційні загрози та знизити вразливість критичної інфраструктури, а також прийняти належні заходи для запобігання й зменшення їх впливу [3].

2. Розроблення та впровадження заходів безпеки, включаючи фізичний захист, кібербезпеку, контроль доступу до інформації і захист від терористичних атак. Це можуть бути як системи моніторингу, так і системи виявлення вторгнень, резервне живлення та резервні мережі зв'язку.

3. Розроблення планів відновлення та впровадження механізмів для швидкого усунення негативних наслідків у разі виникнення кризових ситуацій. Ця компонента передбачає резервування необхідних ресурсів, проведення тренувань і випробувань планів відновлення, а також співпрацю з іншими секторами та органами влади для координації зусиль.

4. Свідомість і навчання. Ця компонента включає проведення навчальних семінарів, тренувань, кампаній з інформування про можливі небезпеки і загрози.

5. Забезпечення ефективного співробітництва між різними секторами, органами влади, операторами та іншими зацікавленими сторонами. Ця компонента забезпечує обмін інформацією, спільне планування, взаємодію та координацію дій у разі надзвичайних ситуацій.

Ефективне співробітництво на ринку електротехнічного обладнання між різними сторонами допомагає обмінюватися важливою інформацією, координувати реагування та відновлення після настання певних кризових ситуацій, а також спільно розробляти стратегію забезпечення резильєнтності. Це може бути досягнуто шляхом створення міжсекторальних комітетів або робочих груп, які об'єднують представників різних секторів та органів влади для формування стратегій співробітництва, обміну інформацією про стан інфраструктури, загрози та інші важливі питання.

Крім того, співробітництво повинно включати спільне планування й сумісні дії операторів ринку і виробників електротехнічного обладнання з виявлення та реагування на небезпеку. Це дозволяє сторонам взаємодіяти, вирішувати складні ситуації та організовувати свої плани і процедури. Такі дії допомагають виявляти «вузькі» місця, вдосконалювати спільні процеси, формувати складські запаси готової продукції, приймати ефективні рішення щодо проведення планових та аварійних ремонтних робіт, а також покращувати комунікацію і взаєморозуміння між операторами та виробниками електротехнічного обладнання. Дане співробітництво є важливим фактором у забезпеченні резильєнтності критичної інфраструктури, оскільки воно дозволяє поєднати ресурси компаній та зусилля сторін для ефективного управління й реагування на загрози та кризові ситуації. Крім того, таке співробітництво допомагає покращити обмін інформацією між замовником та виробником, дає глибоке розуміння

поточної ситуації та є основою для прийняття обґрунтованих рішень з розробки нової техніки і вдосконалення існуючої номенклатури. Для досягнення успішного співробітництва необхідно ідентифікувати механізми комунікації, спільні протоколи і процедури, які дозволяють операторам ринку і виробникам електротехнічної апаратури ефективно співпрацювати та взаємодіяти.

До прикладу, приведу дослідження по українського виробника ТзОВ «ВС РЗВА», яке виробляє високовольтну апаратуру класу напруги 10-110кВ. Основним питанням комунікацій з операторами ринку з початку широкомасштабної війни в Україні стало питання можливості виготовлення обладнання та запчастин до нього на вимогу замовників для оперативного проведення аварійних ремонтів у разі настання кризових ситуацій. Фактично у 2022 році взаємодія між операторами ринку та виробниками електротехнічного обладнання базувалась на побудованих раніше взаємовідносинах з чітким розумінням, яке обладнання буде найбільш затребуваним для забезпечення аварійного відновлення об'єктів енергетичної інфраструктури. Разом з тим, ТзОВ «ВС РЗВА» за власний кошт сформувало резервний фонд готового обладнання та запчастин до нього на випадок проведення аварійних ремонтних робіт з відновлення пошкодженого обладнання замовника. Такі заходи були організовані та запроваджені безпосередньо за участі керівників компанії.

За результатами співпраці було сформовано конструкторські рішення щодо зміни підходів підприємства до питань забезпечення можливостей ремонту обладнання (поточного, аварійного) безпосередньо на об'єктах енергетичної інфраструктури у замовників. Для цього конструкторською та сервісною службою підприємства були розроблені нові технічні рішення та регламенти, які сприяли проведенню швидкого аварійного ремонту пошкодженого обладнання у випадку настання надзвичайних ситуацій безпосередньо експлуатаційними службами замовників.

Вищевикладене дозволяє стверджувати, що успішне співробітництво між секторами інфраструктури, органами влади, операторами та виробниками електротехнічного обладнання зможе значно покращити резильєнтність критичної енергетичної інфраструктури, допоможе уникнути негативних наслідків від небезпечних ситуацій та сприяти швидкому відновленню після кризових подій.

1. Пирожков С.І., Хамітов Н.В. Цивілізаційний проект України: від амбіцій до реальних можливостей. *Вісник Національної академії наук України*. - 2016. - N6. - С. 45-52.
2. Льюїс Т.Г. Захист критичної інфраструктури у сфері внутрішньої безпеки: захист мережевої нації. - 2019. - 464 с.
3. Хаймес Я.Й., Сейдж Е.П. Моделювання, оцінка та управління ризиками. - 2015. - 720 с.

Г.П. Костенко, О.В. Згуровець, В.О. Артемчук

ОСНОВНІ АСПЕКТИ РЕЗИЛЬЄНТНОСТІ ІНФРАСТРУКТУРИ ЕЛЕКТРОЕНЕРГЕТИЧНОГО КОМПЛЕКСУ

Забезпечення резильєнтності систем є однією з головних тенденцій у світі для забезпечення безпеки як критичної інфраструктури, так і національної безпеки в цілому. У контексті безпеки критичної інфраструктури в умовах війни в Україні можна визначити мету забезпечення безпеки та стійкості країни через посилення захисту національної критичної інфраструктури шляхом запобігання, стримування, нейтралізації або пом'якшення наслідків цілеспрямованих дій країни-агресора, спрямованих на знищення, виведення з ладу або експлуатацію критичної інфраструктури. План дій для досягнення цієї мети має передбачати посилення національної готовності, своєчасне реагування та швидке відновлення критичної інфраструктури у разі атаки, стихійного лиха або інших надзвичайних ситуацій [1].

Основною властивістю резильєнтної системи є її здатність до ефективної дії протягом усіх етапів кризового реагування з метою виконання цільових функцій. Як зазначається в [2] через своє економічне, гуманітарне і геополітичне значення об’єкти енергетичної інфраструктури є особливо частими цілями російської агресії. Тому у контексті резильєнтності електроенергетичного комплексу, ця концепція може бути визначена як його здатність витримувати порушення роботи та продовжувати надавати доступні енергетичні послуги споживачам. Стійка енергетична система здатна швидко відновлюватися від руйнівних подій і пропонувати альтернативні способи задоволення потреб енергетичних послуг у разі зміни зовнішніх умов.

У широкому розумінні резильєнтність критичної інфраструктури - це здатність зменшувати масштаб та/або тривалість руйнівної події. Таким чином, під резильєнтністю електроенергетичного комплексу ми розуміємо його здатність забезпечувати потреби споживачів у послугах (електроенергії) незалежно від обставин. Це означає, що система здатна надійно функціонувати у нормальних умовах, протистояти загрозам, адаптуватися до умов, що постійно змінюються, і швидко відновлюватися після реалізації будь-яких загроз (атак, руйнування, тощо).

На рис.1 представлено життєвий цикл резильєнтності, розроблений у [3]. Він містить різні етапи планування та управління резильєнтністю, включаючи цикл зворотного зв’язку для врахування досвіду від уроків, отриманих із попередніх подій. Ця ілюстрація підкреслює, що резильєнтність є більше ніж надійність чи здатність до відновлення. Резильєнтність передбачає планування і пом'якшення цих подій до, під час і після їх виникнення.

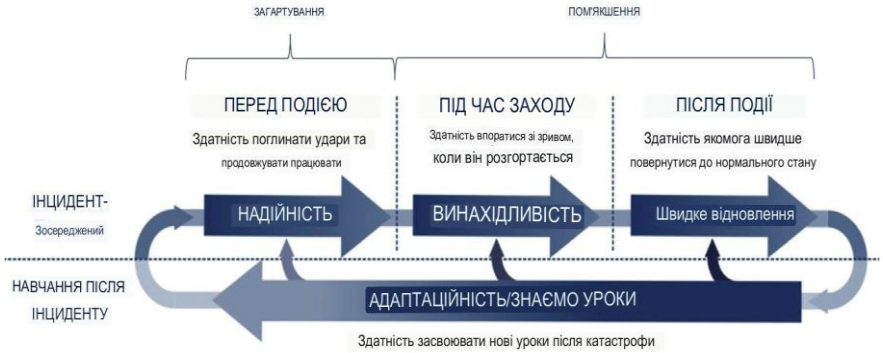


Рисунок 1 – Життєвий цикл резильєнтності [3]

В ідеалі електроенергетичний комплекс повинен мати таку структуру та організацію, щоб володіти властивостями пружності: гнутися без руйнування, виходити з ладу з мінімальними пошкодженнями та забезпечувати швидке відновлення.

1. Практика реагування на руйнівні події в енергетичному секторі.

Поточним законодавством України передбачені заходи для залучених суб'єктів управління та господарської діяльності електроенергетики з метою реагування на кризові ситуації. У разі загрози стійкості функціонування енергетичної системи України, Кабінет Міністрів України, згідно з встановленим законодавством, вводить тимчасові "надзвичайні заходи" для функціонування енергоринку [4,5]. Критеріями для введення таких заходів є:

1) Пошкодження електроенергетичних установок або незаконне втручання третіх осіб, що можуть призвести до обмеження споживання електричної енергії більш як на 100 МВт.

2) Зниження резерву енергогенеруючих потужностей енергетичної системи України нижче допустимого рівня протягом трьох діб.

3) Критичний стан забезпечення паливом, зокрема зниження запасів палива на окремих теплових електростанціях енергогенеруючих компаній нижче 20-денного запасу.

4) Відсутність протягом трьох місяців підряд повної оплати електричної енергії або оплата нижче 90 відсотків в розрахунковому місяці.

Рішення про вжиття тимчасових надзвичайних заходів приймає Кабінет Міністрів України на підставі подання Міненерговугілля або НКРЕКП. Тимчасові надзвичайні заходи можуть бути введені на період, що у мирний час не перевищує одного місяця. Протягом цього періоду суб'єкти електроенергетики, незалежно від форми власності, зобов'язані діяти відповідно до стандартів операційної безпеки енергетичної системи України та оперативних команд і розпоряджень Оператора системи передачі "НЕК "Укренерго". Вимоги щодо забезпечення безпеки об'єктів електроенергетики

в надзвичайних ситуаціях є обов'язковими для всіх суб'єктів ринку електричної енергії, незалежно від форми власності.

2. Система автоматичного регулювання частоти і потужності

Частота є одним з ключових параметрів, що визначають якість електричної енергії і режим роботи енергосистеми. Забезпечення стабільності та надійності роботи енергосистеми визначається балансом між виробленою та спожитою активною потужністю у кожен момент часу [6]. Порушення балансу потужності призводить до зміни частоти, тому регулювання частоти в енергосистемі застосовується для її відновлення і підтримки в межах допустимих значень. Регулювання частоти є важливим елементом керування режимами роботи енергосистеми, оскільки безпосередньо впливає на стабільність та надійність її функціонування і є важливим показником резильєнтності енергосистеми.

3. Сегментація та резервування інфраструктури

Вихід компонентів з ладу є частим наслідком руйнівних подій. Під час екстремальних умов імовірність одночасного виходу декількох компонентів з ладу також збільшується. Однією з ключових ознак резильєнтності є обмеження наслідків для ОЕС в умовах відмов багатьох окремих компонентів. Це може бути досягнуто за допомогою резервування, запобігання послідовностям каскадних відмов та проектування системи з можливістю плавного зниження потужності при відмовах кількох окремих компонентів. Існують різні стратегії для зменшення критичності окремих елементів інфраструктури електроенергетичного комплексу. Одна з таких стратегій - сегментація. Наприклад, шина на підстанції може бути розділена на секції, з'єднані вимикачем, щоб у разі виникнення несправності або короткого замикання в одній секції, необхідно відключити лише цю секцію без відключення інших. Резервування є найпоширенішим методом обмеження наслідків від відмови обладнання, однак слід відзначити, що це супроводжується значними витратами. Так, може бути кілька підстанцій в одній області, кожна з яких обслуговує частину навантаження в регіоні або громаді, з альтернативними маршрутами доставки електроенергії до різних частин системи. Часто в одній області прокладені декілька ліній передачі різної напруги. Наприклад, наявність основної високовольтної лінії передачі не означає, що це єдиний спосіб доставки електроенергії в регіоні, оскільки також може бути присутня інфраструктура передачі іншої напруги. Для забезпечення надійності електропостачання можуть використовуватися дублюючі лінії електропередачі від різних підстанцій.

4. Розвиток розподіленої генерації

Зменшення критичності енергогенеруючих установок можливе шляхом диверсифікації шляхів постачання палива, а також розвитку відновлюваних джерел енергії, які не потребують викопного палива. Розвиток розподіленого генерування енергії для зменшення залежності від централізованого виробництва електроенергії також може збільшити резильєнтність системи енергозабезпечення, особливо для віддалених районів та у разі використання різних джерел енергії. Упродовж останніх кількох років відбувається значне

зростання розподіленого виробництва електроенергії, включаючи виробництво електроенергії домашніми СЕС на ділянках споживачів в багатьох регіонах України [7]. Ці тенденції в основному обумовлені економічними чинниками, але також дають значні переваги з точки зору стійкості, якщо ці енергогенеруючі активи можуть працювати незалежно від вимог напруги та частоти централізованої енергосистеми.

5. Розвиток систем зберігання енергії

Накопичення енергії є перспективним способом не тільки для зберігання енергії, а також для підвищення якості електричної енергії та надійності розподільчих мереж. Слід зазначити, що ефективність функціонування систем накопичення енергії (СНЕ) в системі електропостачання значно підвищується за рахунок можливості поєднання в них кількох функцій [8]. Вони можуть використовуватися не лише для накопичування та зберігання енергії (тривалого чи короткострокового), але й для надання енергосистемі ряду додаткових послуг, які здатні значно підвищити керованість енергосистеми. Так, СНЕ можуть залучатися до стабілізації частоти, регулювання напруги та реактивної потужності, забезпечення відновлення функціонування ОЕС України після системних аварій [4]. Таким чином розвиток та впровадження СНЕ в енергосистему сприятиме забезпеченню стабільності, надійності та ефективності функціонування енергосистеми, а також розвитку та інтеграції відновлюваних джерел енергії, та дозволить підвищити її резильєнтність.

6. Безпечні комунікації

У сучасних системах електропостачання комунікації стали важливим та незамінним компонентом забезпечення їх нормального функціонування. В минулому проектування електроенергетичної інфраструктури виконувалось з метою мінімізації залежності від комунікацій, через їх високу вартість та невисоку надійність. Однак, з розвитком різних форм комунікацій протягом останніх десятиліть, залежність від них значно збільшилась на всіх рівнях електропостачання. Один з прикладів такої залежності від комунікацій - це системи ринку (електроенергії, допоміжних послу, тощо), які можуть значно погіршити надійність роботи енергетичної системи в разі виникнення порушень зв'язку. Хоча цю залежність було зменшено за допомогою резервування та створення надійних комунікаційних, все ж існує ризик в сценаріях, коли функціонування комунікаційних систем буде обмежено. Також до ризиків можна віднести питання, що пов'язані з кібербезпекою та різними формами кібернетичних атак на комунікаційну інфраструктуру. Саме тому є важливим як вжиття посилених заходів з кібернетичної безпеки, так і розробка стратегій функціонування електроенергетичного комплексу в разі відсутності комунікації.

Висновки

Електроенергетичний комплекс є частиною критичної інфраструктури, епіцентром та рушійною силою економіки, національної безпеки та екологічної ситуації в країні. Він взаємопов'язаний з іншими компонентами критичної інфраструктури, такими як газо- та водопостачання, транспортні та

комунікаційні системи. Збій в системі енергопостачання безпосередньо і значною мірою впливає на функціонування цих компонент критичної інфраструктури. Таким чином, підвищення резильєнтності енергетичного комплексу вкрай необхідно для забезпечення безперервної роботи критичної інфраструктури загалом.

Найбільш необхідними та перспективними підходами до підвищення резильєнтності енергосистеми є розробка відповідної нормативної бази, використання системи автоматичного регулювання частоти і потужності, забезпечення ресурсодостатності (в тому числі резервування технічних компонент), розвиток розподіленої генерації, інтеграцію систем накопичення енергії в енергосистему, підсилення кібербезпеки.

Виконання цих підходів дозволять підвищити здатність енергетичного комплексу до самовідновлення, та стійкість у руйнівних екстремальних ситуаціях, які виходять за рамки рядових відмов.

1. Павленко, О., Антоненко, А., Ніцович, Р., Євтушок, С., & Суходоля, О. (2022). *Оцінка стійкості енергетичної інфраструктури України.* Діксі Груп.
2. Артемчук, В. (2022). *Перспективи розроблення методів і засобів забезпечення резильєнтності об'єктів енергетичної галузі України.* URL: https://www.researchgate.net/publication/365769552_Perspektivi_rozroblenna_metodiv_i_zasobiv_zabezpecenna_rezilentnosti_ob%27ektiv_energeticnoi_galuzi_Ukraini
3. Moteff, J.D. (2012). *Critical infrastructure resilience: the evolution of policy and programs and issues for congress.* Congressional Research Service, R42683.
4. Закон України *«Про ринок електричної енергії України».* URL: https://zakon.rada.gov.ua/laws/show/2019-19#Text
5. Кабінет Міністрів України. (2014). Постанова від 13 серпня 2014 р. № 372 *«Про затвердження Порядку вжиття тимчасових надзвичайних заходів з подолання наслідків тривалого порушення нормальної роботи ринку електричної енергії».* URL: http://zakon5.rada.gov.ua/laws/show/372-2014-%D0%BF
6. Kulyk, M., & Zgurovets, O. (2020). *Modeling of power systems with wind, solar power plants and energy storage.* In Systems, Decision and Control in Energy I. Studies in Systems, Decision and Control, vol. 298. Springer, Cham. https://doi.org/10.1007/978-3-030-48583-2_15
7. Костенко, Г., & Згуровець, О. (2023). *Сучасний стан та перспективи розвитку відновлюваної розподіленої генерації в Україні.* Системні дослідження в енергетиці, 2 (73), 4-17. https://doi.org/10.15407/srenergy2023.02.004
8. Костенко Г.П., & Згуровець О.В. (2023). *Можливості підвищення керованості енергосистеми шляхом використання систем накопичення енергії.* XXIV Міжнародна Науково-Практична Онлайн – Конференція «Відновлювана енергетика та енергоефективність у XXI столітті», Інститут відновлюваної енергетики НАН України, Київ.

О.В. Згуровець, Г.П. Костенко

ЗАСТОСУВАННЯ МІКРОМЕРЕЖ ДЛЯ ПОКРАЩЕННЯ РЕЗИЛЬЄНТНОСТІ ЕНЕРГЕТИЧНИХ СИСТЕМ

Електроенергетична система відіграє критичну роль у функціонуванні економіки та безпеки країни, знаходячись у тісному зв'язку з іншими важливими інфраструктурами, включаючи газопостачання, водопостачання, транспорт та телекомунікації. Підтримка стабільного електропостачання є вирішальною для безперебійної роботи цих систем. Інтеграція локальних мереж, або мікромереж, у загальну енергосистему є одним зі способів підвищення її резильєнтності [1]. Локальні мережі мають здатність до самовідновлення та демонструють стійкість навіть у випадках, коли відбуваються надзвичайні події, що виходять за межі звичайних відмов. Гнучкість та керованість локальних мереж роблять їх ефективним рішенням для покращення стійкості енергосистеми. Роль мікромереж у забезпеченні резильєнтності енергосистем є важливою темою для дослідження, з огляду на їх потенціал та обмеження.

Електромережа чутлива до збурень та руйнувань, що можуть викликати масштабні відключення споживачів електроенергії. Статистичні дані вказують, що приблизно 90% відключень відбуваються через проблеми в системі розподілу, тому особливий фокус в дослідженнях направлений на резильєнтність розподільчих мереж.

Мікромережі мають здатність працювати незалежно від централізованої енергосистеми і демонструють великий потенціал для швидкого реагування на військові, екологічні та антропогенні кризи. Більшість існуючих мікромереж мають обмежену масштабність і працюють за моделлю, в якій один оператор управляє мережею та може обслуговувати різноманітні джерела енергії та споживачів. Ці мікромережі можуть поєднувати як джерела традиційної так і відновлюваної енергії відносно невеликої потужності, а також системи зберігання енергії.

У науковій літературі не існує універсального визначення резильєнтності, цей термін широкий і включає багато факторів [1-3]. Його можна описати як здатність ефективно готуватися до подій з низькою ймовірністю, але з великим потенціалом збитків, протистояти цим подіям, зменшувати їх негативні наслідки та/або скорочувати тривалість періоду відновлення. Це включає здатність переживати кризу, адаптуватися до неї, визначати невизначеності та швидко відновлюватись після таких подій.

Резильєнтність енергосистеми можна поділити на дві основні категорії: 1) резильєнтність інфраструктури та 2) операційну (експлуатаційну) резильєнтність. Резильєнтність інфраструктури визначається в основному як міцність фізичного рівня енергетичної системи протистояти і бути менш сприйнятливим до пошкодження внаслідок великих збоїв. Операційна резильєнтність стосується безперервності роботи, тобто безперебійного

постачання або достатності готових для використання генеруючих потужностей, незважаючи на негативні події.

Характеристики резильєнтності інфраструктури включають такі аспекти, як стійкість, надійність, резервування, а також швидкість реагування та відновлення, як це представлено на рис. 1. Стійкість фокусується на посиленні компонентів, надійність зосереджується на проектуванні компонентів для роботи в різних умовах, резервування включає встановлення резервних компонентів, а швидкість реагування та відновлення стосуються того, наскільки швидко та ефективно система реагує під час збою [4].

Рисунок 1 – Основні характеристики резильєнтності енергосистеми [4]

Традиційна централізована енергосистема, яка відносно проста у управлінні та експлуатації, може мати меншу надійність в порівнянні з розподіленою генерацією, оскільки може бути вразливою до збоїв у окремих її вузлах. Водночас, переваги розподілених енергетичних ресурсів [5] та потенційні переваги архітектури мікромереж, а також стратегії розподіленого керування, привертають все більше уваги у контексті підвищення безпеки та резильєнтності мережі.

Сучасні енергетичні системи реалізуються шляхом комбінації різних технологій, включаючи сонячну енергію, вітрову енергію, накопичувачі енергії, електромобілі, розумні будівлі та активних користувачів. Всі ці елементи можуть бути об'єднані в мікромережі, які можуть працювати в режимі острів, а також у паралельному режимі з основною мережею. Інтеграція мікромереж із інтелектуальними датчиками та системами керування енергією дозволяє ефективно інтегрувати ці системи на рівнях

низької та середньої напруги в наявні розподільчі мережі, забезпечуючи їх ефективну, надійну та економічну роботу.

Підвищення резильєнтності вимагає розробки ефективних стратегій пом'якшення, що сприятимуть швидкому відновленню системи під час критичних подій. Ці вимоги можуть бути забезпечені шляхом інтеграції автономних мікромереж, які Міжнародна електротехнічна комісія (IEC) визначає як «сукупність керованих розподілених генераторів і ресурсів навантаження, розташованих поблизу один від одного, що складається з кількох джерел змінного струму, серед яких принаймні одне відновлюване джерело енергії, таке як вітер або сонце» [6].

Локальні мікромережі заклали основу інтелектуальних мереж, надавши можливість створення самоконтрольованої енергосистеми, яка здатна через організацію взаємозв'язку між розподіленими енергетичними ресурсами та регульованими навантаженнями надійно працювати в межах визначених електричних параметрів.

Мікромережі використовуються для оптимізації різноманітних аспектів функціонування енергетичних систем, що відображено на рис. 2, де показана класифікація різних функцій мікромереж з огляду на покращення резильєнтності енергосистем.

Рисунок 2 – Функції мікромереж для підвищення резильєнтності енергосистеми [7]

Мікромережі надають значну перевагу у підвищенні резильєнтності енергосистеми, впроваджуючи різноманітні стратегії – від планування реагування на надзвичайні ситуації до гарантованого надійного енергопостачання споживачів. Забезпечення надійності енергосистеми відбувається на різних рівнях – починаючи від фізичного зміцнення компонентів системи та оперативного відновлення послуг, і закінчуючи розробкою стратегій управління, що підсилюють стійкість енергосистеми.

Висновки

В ході дослідження була проаналізована роль мікромереж у підвищенні резильєнтності енергетичних систем. Розглянуто визначення та характеристики резильєнтності енергетичних систем. Крім того, узагальнено функції мікромереж, які сприяють підвищенню стійкості енергетичних систем, такі як відновлення обслуговування, стратегії формування мережі, контроль і стабільність, а також запобіжні заходи.

Виявлено, що локальні мікромережі володіють значним потенціалом підвищення резильєнтності енергоситеми шляхом реалізації різноманітних стратегій, від планування реагування на надзвичайні ситуації до забезпечення надійного енергопостачання споживачів. Однак, необхідно провести подальші дослідження для визначення оптимальних стратегій впровадження та управління мікромережами.

1. Moteff, J. D. (2012). *Critical infrastructure resilience: The evolution of policy and programs and issues for congress.* Congressional Research Service, R42683.
2. Sepúlveda-Mora, S. B., & Hegedus, S. (2022). *Resilience analysis of renewable microgrids for commercial buildings with different usage patterns and weather conditions.* Renewable Energy, 192, 731-744. https://doi.org/10.1016/j.renene.2022.04.090.
3. Strbac, G., Hatziargyriou, N., Lopes, J. P., Moreira, C., Dimeas, A., & Papadaskalopoulos, D. (2015). *Microgrids: Enhancing the Resilience of the European Megagrid.* IEEE Power and Energy Magazine, 13(3), 35-43. https://doi.org/10.1109/MPE.2015.2397336.
4. Cabinet Office. (2011). *Keeping the Country Running: Natural Hazards and Infrastructure*.
5. Костенко, Г., & Згуровець, О. (2023). *Сучасний стан та перспективи розвитку відновлюваної розподіленої генерації в Україні.* Системні дослідження в енергетиці, 2(73), 4-17. https://doi.org/10.15407/srenergy2023.02.004.
6. International Electrotechnical Commission. (2014). *Microgrids for disaster preparedness and recovery: With electricity continuity plans and systems.*
7. Bajwa, A. A., Mokhlis, H., Mekhilef, S., & Mubin, M. (2019). *Enhancing power system resilience leveraging microgrids: A review.* Journal of Renewable and Sustainable Energy, 11(3), 035503. https://doi.org/10.1063/1.5066264.

В.С. Коберник

СОНЯЧНЕ ТЕПЛОПОСТАЧАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В умовах війни в Україні в рамках підготовки до наступного опалювального сезону важливими є інноваційні рішення для об'єктів критичної інфраструктури, до яких відносяться системи теплопостачання.

В Україні річне надходження сонячного випромінювання знаходиться на одному рівні з країнами, які активно використовують сонячні колектори (Німеччина, Нідерланди, Австрія та ін.). Вся територія України є придатною для розвитку систем сонячного теплопостачання і гарячого водопостачання, але ці можливості не розвиваються.

Сонячні колектори добре нагрівають воду влітку, коли яскраве сонце і тривалий світловий день. Зимою вони використовуються як додаткове джерело теплопостачання. Є літні та зимові колектори. Тепловим агентом у літніх системах є вода, а у зимових – антифриз. Літні колектори мають один контур, а цілорічні – два, працюють разом з основним джерелом тепла.

В Україні є мало досліджень по сонячному теплопостачанню. Це роботи Інституту відновлюваної енергетики НАН України, наприклад [1, 2]. Аналіз досвіду застосування систем сонячного теплопостачання і гарячого водопостачання, що працюють у світі [3, 4], є цінним при впровадженні аналогічних систем в Україні. Міністерство інфраструктури у травні 2023 р. оголосило про початок відбору проектів, фінансування яких може здійснюватися в рамках фінансової угоди «надзвичайна кредитна програма для відновлення України» між Україною та Європейським інвестиційним банком (ЄІБ). Проекти з сонячного теплопостачання збільшують надійність теплопостачання і можуть бути важливими для відновлення критичної інфраструктури країни.

Для систем теплопостачання показником економічності є LCOH (levelised cost of heat generation) – це середня собівартість виробництва теплової енергії за життєвий цикл, що враховує всі витрати. Для сонячної енергії паливних та екологічних складових витрат немає, тому середня собівартість теплової енергії обчислюється за формулою:

$$\mathrm{LCOH} = \frac{I_0 + \sum_{t=1}^{n} \frac{M_t}{(1+r)^t}}{\sum_{t=1}^{n} \frac{Y_t}{(1+r)^t}}$$

де: LCOH – середня собівартість виробництва теплової енергії протягом терміну роботи, дол. США/кВт·год;

t – роки з початку спорудження;

n – життєвий цикл, роки;

I_0 – інвестиційні витрати, дол. США;

M_t – експлуатаційні витрати, пов'язані з обслуговуванням, дол. США/рік;

Y_t – виробництво теплової енергії МВт·год/рік;

$Y_t = Q \times \tau$;

Q – теплова потужність, $МВт_т$;

τ – час роботи, год./рік;

r – дисконтна ставка.

У цій роботі розрахована собівартість виробництва теплової енергії за життєвий цикл. Вихідні данні. Потужність сонячної системи Q = 1 $МВт_т$. Експлуатаційні витрати приймаються [5]: 0,5% від інвестиційних витрат при площі більше 1000 м² і 1% при меншій площі.). Середньомісячне значення коефіцієнта використання встановленої потужності (КВВП) для СЕС України за 2020-2021 роки становило 14,1% [6], тому час роботи τ_1 = 1235 год/рік. Термін роботи n = 25 років. Дисконтна ставка змінюється від 10% до 25%.

Європейські сонячні панелі виробляються із застосуванням інноваційних галузевих технологій, надійні та стійкі до навантажень. За даними роботи [5] середньоєвропейські інвестиційні витрати на системи сонячного теплопостачання потужністю 1000 $кВт_т$ у 2020 році складали 815 дол. США/$кВт_т$. За результатами розрахунків середні собівартості виробництва теплової енергії протягом життєвого циклу системи сонячного теплопостачання склали (дол. США/кВт·год): 0,0809 (r = 10%); 0,1116 (r = 15%); 0,1439 (r = 20%); 0,1768 (r = 25%).

В програмі Excel отримана апроксимаційна залежність середньої собівартості виробництва теплової енергії (в дол. США/кВт·год) за життєвий цикл від дисконтної ставки для потужності 1 $МВт_т$:

$$LCOH = 0{,}6398 \times r + 0{,}016$$

Для порівняння з тарифами на теплову енергію в Україні за курсом НБУ 1 дол. США = 36,5686 грн. розрахункові середні собівартості теплової енергії були перераховані у грн./Гкал : 3440,8 (r = 10%); 4746,52 (r = 15%); 6120,3 (r = 20%); 7519,57 (r = 25%).

Середня собівартість виробництва теплової енергії обернено залежить від кількості годин роботи: $LCOH_2 = LCOH_1 / (\tau_2 / \tau_1)$. Якщо кількість годин роботи збільшиться у 2 рази (наприклад для південних регіонів), то LCOH зменшиться також у 2 рази.

За даними «Київтеплоенерго» [7] тарифи на централізоване теплопостачання у осінньо-зимовий період 2022-2023 рр. складали (грн./Гкал): для бюджетних організацій 4235,72 (протягом дії воєнного стану 2732,04, компенсація згідно закону [8]), для інших організацій 6416,14 (тариф протягом дії воєнного стану 2876,71, компенсація згідно закону [8]). З

порівняння видно, що тарифи централізованого теплопостачання для бюджетних організацій є нижчими ніж сонячного теплопостачання за дисконтних ставок 15%, 20% і 25%, а для інших організацій за дисконтної ставки 25%.. Але важливим моментом є автономність постачання тепла та гарячої води.

Висновки

Значний вплив на середню собівартість виробництва сонячної теплової енергії мають питомі інвестиційні витрати на встановлення, кількість годин роботи та дисконтна ставка.

В Україні можливо в короткий термін організувати забезпечення об'єктів критичної інфраструктури тепловою енергією від використання сонячних технологій. Перспективним напрямком є використання систем сонячного теплопостачання у комбінації іншими джерелами теплової енергії, наприклад з тепловими насосами.

Отримані показники сонячного теплопостачання можуть бути використані в програмах щодо розвитку теплопостачання об'єктів критичної інфраструктури в Україні.

1. Матях С.В., Суржик Т.В., Рєзцов В.Ф., Іванчук В.Ю. Напрями та перспективи розвитку сонячної теплоенергетики // Відновлювана енергетика, 2021, № 3, с. 33—44. https://doi.org/10.36296/1819-8058.2021.3(66).33-44
2. Зощенко С.А. Сонячне теплопостачання: різновиди систем перетворення, ефективність // Відновлювана енергетика, 2022, № 2, с. 43—48. https://doi.org/10.36296/1819-8058.2022.4(71)43-48
3. Гламаздін Павло, Кірєєв Ейтан. Перспективи використання досвіду Ізраїлю в сонячному гарячому водопостачанні в Україні // Енергоефективність в будівництві та архітектурі, 2019, вип. 13, с. 69—78. https://doi: 10.32347/2310-0516.2019.13.69-78
4. Renewable power generation costs in 2020. IRENA, June 2021. – 180 p. URL: https://www.irena.org/publications/2021/Jun/Renewable-Power-Costs-in-2020
5. Bärbel Epp. Cost and market trends in solar industrial heat. 2021. 22 p. URL: https://www.dlr.de/sf/en/PortalData/73/Resources/dokumente/soko/soko2021/DLR-SolarColloquium2021_Cost_and_market_trends_EPP.pdf
6. Сидоров Дмитро. Изменчивое солнце и попутный ветер // Енергобізнес, 2022, № 6. URL: https://e-b.com.ua/izmencivoe-solnce-i-poputnyi-veter-3299
7. Тарифи на теплову енергію КП «Київтеплоенерго». Розпорядження КМВА № 673 від 30.09.2022 року.
8. Закон України «Про особливості регулювання відносин на ринку природного газу та у сфері теплопостачання під час дії воєнного стану та подальшого відновлення їх функціонування» від 29.07.2022 № 2479-IX.

Р.В. Шитлюк

ВИКОРИСТАННЯ СТАНДАРТІВ NIST ДЛЯ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ АКТИВІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Закон України № 1882-IX «Про критичну інфраструктуру» [1] від 16 листопада 2021 року визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки.

Згідно статті 11. даного закону, повинен бути сформований реєстр об'єктів критичної інфраструктури. Проте сам порядок формування реєстру було затверджено лише від 28 квітня 2023 р. постановою № 415 Кабінету міністрів України [2].

Оскільки на період воєнного стану безпосередній доступ до інформації, що міститься в Реєстрі об'єктів критичної інфраструктури (далі - Реєстр), в тому числі до інформації, яка розміщується на офіційному веб-сайті уповноваженого органу у сфері захисту критичної інфраструктури України, є обмеженим – орієнтовна їх кількість станом на даний момент невідома.

Незалежно від кількості таких об'єктів – необхідно забезпечити належний їх захист. 29.05.2023 Державна служба спеціального зв'язку та захисту інформації України опублікувала наказ № 463 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами» [3]. Даний документ розроблений з врахуванням стандартів NIST (Національного інституту стандартів і технології США) та визначає наступне:

- вимоги до кіберзахисту АСУ ТП (зокрема – SCADA-систем), порядок їх впровадження та підтвердження виконання;
- загальну систему дій щодо проєктування, впровадження, підтримки та постійного вдосконалення кіберзахисту автоматизованих систем управління технологічними процесами;
- мінімальні рівні впровадження стандартного цільового профілю кіберзахисту для об'єктів критичної інфраструктури I рівня (катастрофічні наслідки) та II рівня (критичні наслідки) негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури.

Дані рекомендації є у відкритому доступі та можуть бути використані будь-якими компаніями для підвищення рівня зрілості інформаційної безпеки.

Проте, далеко не всі об'єкти критичної інфраструктури використовують саме системи типу АСУ ТП, тому дані рекомендації можуть бути не зовсім релевантними.

Як базис для подальшої розробки загальних рекомендацій щодо підвищення рівня зрілості інформаційної безпеки об'єктів критичної інфраструктури доцільним вектором розвитку є подальше використання стандартів NIST в якості базових рекомендацій з подальшим врахуванням реалій поточного стану кібербезпеки в Україні.

Окрім вищевказаної, наступні причини дозволяють вважати NIST одною з кращих методологічних баз кібербезпеки для критичної інфраструктури:

- Широке визнання: NIST отримав широке визнання та прийняття як у державному, так і в приватному секторах. Його широке використання підвищує сумісність і полегшує співпрацю між урядовими установами, а також з міжнародними галузевими партнерами.

- Підхід, що ґрунтується на оцінці ризиків: у структурі підкреслюється перспектива управління ризиками, що дозволяє урядовим організаціям виявляти, оцінювати та визначати пріоритетність ризиків кібербезпеки на основі їх потенційного впливу на критично важливі послуги та операції. Він сприяє проактивному та безперервному циклу оцінки ризиків, пом'якшення ризиків і постійного моніторингу.

- Гнучкість і масштабованість: стандарти NIST розроблено таким чином, щоб бути адаптованим до різноманітних організацій, незалежно від їх розміру, сектору чи рівня зрілості кібербезпеки. Він надає набір добровільних інструкцій і найкращих практик, які можна адаптувати до конкретних організаційних потреб, дозволяючи державним організаціям узгоджувати свої зусилля з кібербезпеки зі своїми унікальними вимогами та ресурсами.

- Ядро фреймворку: Ядро фреймворку — це набір дій із кібербезпеки, організованих у п'ять одночасних і безперервних функцій: ідентифікація, захист, виявлення, реагування та відновлення. Ця структура дозволяє державним організаціям розробити цілісний і інтегрований підхід до кібербезпеки, враховуючи різні аспекти, такі як оцінка ризиків, контроль безпеки, реагування на інциденти та безперервність бізнесу.

- Співпраця та комунікація: NIST заохочує співпрацю та комунікацію між різними зацікавленими сторонами, зокрема державними установами, галузевими партнерами та регуляторними органами. Він сприяє спільному спілкуванню та розумінню ризиків кібербезпеки, полегшуючи обмін інформацією, обмін розвідувальними даними про загрози та координацію заходів реагування.

- Інтеграція зі стандартами та правилами: стандарти NIST узгоджуються з іншими широко визнаними стандартами, рекомендаціями та правилами, такими як ISO 27001, COBIT та ін.. Ця інтеграція дозволяє урядовим організаціям гармонізувати свої практики кібербезпеки та відповідати відповідним вимогам, використовуючи наявні інвестиції в програми відповідності та безпеки.

Додатково, задля підвищення рівня захищеності інформаційних активів об'єктів критичної інфраструктури - NIST дозволяє інтегрувати модель нульової довіри (Zero Trust) [4], яка базується на припущенні, зловмисник вже присутній всередині периметру інформаційної безпеки і що корпоративне середовище нічим не відрізняється (або не є більш надійним), ніж будь-яке середовище, яке не належить підприємству. Згідно з цією парадигмою, підприємство не має припускати довіри та постійно аналізувати й оцінювати ризики для своїх активів і бізнес-функцій, а потім вводити засоби захисту для пом'якшення цих ризиків. У такому випадку засоби захисту зазвичай передбачають мінімізацію доступу до ресурсів (таких як дані та обчислювальні ресурси та програми/сервіси) лише для авторизованих суб'єктів і активів, а також постійну ідентифікацію, автентифікацію та авторизацію кожного запиту на доступ.

1 Закон України «Про критичну інфраструктуру» № 1882-IX (2021). https://zakon.rada.gov.ua/laws/show/1882-20#Text

2 Постанова Кабінету Міністрів України «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» № 415 (2023) https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

3 Наказ Адміністрації Держспецзв'язку від 29.05.2023 № 463 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами» https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami

4 National Institute of Standards and Technology. (August 2020). Zero Trust Architecture https://csrc.nist.gov/publications/detail/sp/800-207/final

І.П. Криворучко

АЛГОРИТМ І МОДЕЛЮВАННЯ ПРИСКОРЕНОГО КУТОВОГО ПЕРЕМІЩЕННЯ РОТОРА КРОКОВОГО ДВИГУНА

Кроковий двигун (КД) використовується у електромеханічних системах, де вимагається точне позиціонування робочого органу, механічно зв'язаного з ротором КД. Основний режим роботи КД – ступінчасте кутове переміщення ротора, яке задається сигналом керування. Через наявність постійних магнітів фіксація положення ротора відбувається навіть у відсутності струмів збудження статорної обмотки. Через інерцію ротора та магнітного зчеплення ротора та статора набуття ротором певної швидкості вимагає деякого часу. Занадто швидке збудження магнітного потоку статора може призвести до втрати керування та пропуску кроків. З метою усунення цих небажаних наслідків і підвищення надійності роботи зазвичай використовують різні алгоритми розгону/гальмування приводу електромеханічних систем. Ці алгоритми відомі як S - подібні криві і можуть описуватися різноманітними математичними залежностями, графічні зображення яких подібні до форми літери S.

Найпростішим способом прискорення/гальмування є лінійна зміна швидкості на ділянках розгону та гальмування (Рис.1). Це так званий трапецеїдальний тип формування прискорення/уповільнення [1].

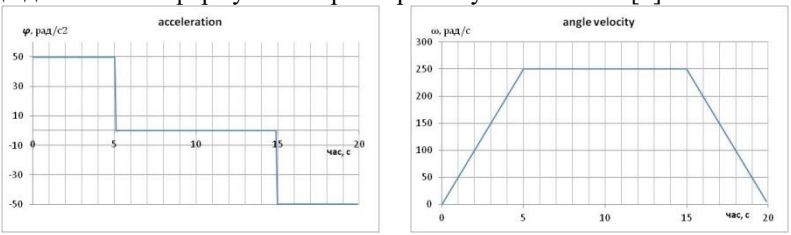


Рис. 1 Діаграми трапецеїдального типу розгону-гальмування

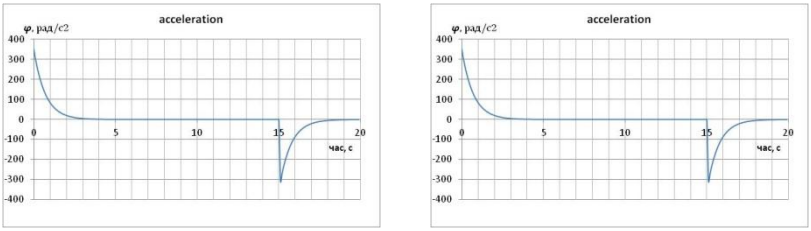
Інший спосіб реалізації розгону/гальмування використовує експоненціальну залежність (Рис.2). На інтервалі прискорення кутова швидкість описується виразом:

$$\omega = \omega_0 (1 - e^{-t/\lambda}), \qquad (1)$$

де ω_0 – відповідає фіксованому значенню кутової швидкості (часовий інтервал: 0 – 5; $\boldsymbol{\lambda}$ – постійна часу, що визначає форму кривої. На ділянці гальмування 15 – 20 швидкість описується іншим рівнянням:

$$\omega = \omega_0 (e^{-t/\lambda}) \qquad (2)$$

Як і для трапецеїдального типу графік залежності для прискорення (Рис.2 (а)) має розриви в початковий момент часу і t_2 = 15с. В [2] пропонується "гнучкий *S*-qurve метод" реалізації прискорення/гальмування.



а б

Рис.2 Діаграми експоненціального типу розгону/гальмування

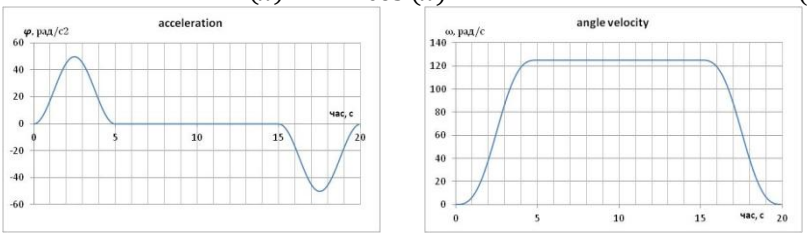
Швидкість представляється у вигляді кубічної поліноміальної функції наступного вигляду:

$$\omega(\alpha) = (a_1 + 2a_2\alpha + 3a_3\alpha^2 + 4a_4\alpha^3)/t_n \qquad (3)$$

де $\alpha = t/t_n$; t_n – час необхідний для здійснення розгону/гальмування.

В представленій роботі пропонується використовувати тригонометричні функції, які нескінченно диференційовані, неперервні і просто розраховуються. Найпростішою для розрахунків і застосування вибрано:

$$F(x) = 1 - \cos(x) \qquad (4)$$



а б

Рис.3 Діаграми косинусного типу розгону/гальмування

Діаграми зміни в часі основних розрахованих вихідних параметрів моделі наведені на Рис.4. На верхньому графіку показано ступінчату зміну величини заданого переміщення та імпульси зчитування цих значень для подальших обрахунків.

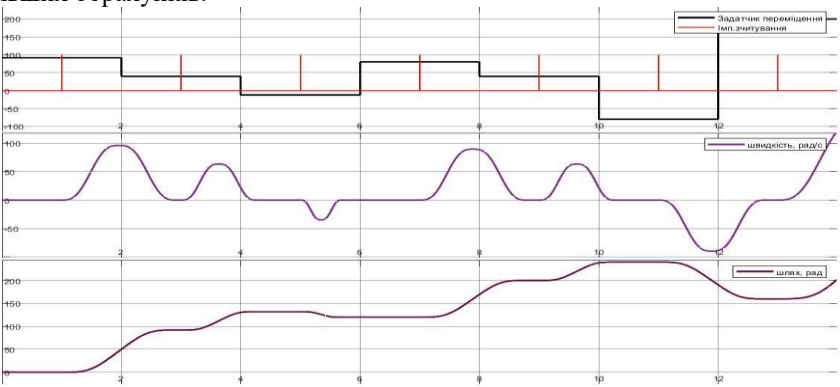


Рис.4 Діаграми зміни швидкості та переміщення за Simulink моделлю косинусного типу розгону/гальмування

Основні параметри, які враховуються у розрахунках швидкості (шляху): L_0 – задане переміщення, $\boldsymbol{\omega}_{\text{m}}$ - максимальна допустима кутова швидкість та $\boldsymbol{\varphi}_{\text{m}}$ – максимальне прискорення.

Висновки

Розроблено алгоритм та ПЗ плавного розгону/гальмування косинусного типу. Для розробки та перевірки запропонованого алгоритму застосовувалося моделювання в імітаційному програмному середовищі MatLab/Simulink. Використання такого типу S-кривої розгону/гальмування виключає появу різких змін швидкості та прискорення – ривків. Це може покращити експлуатаційні режими обладнання, де використовуються КД (та інші керовані електроприводи). На відміну від відомих типів розгону/гальмування, запропонований тип не має розривів у похідній за часом від кутового прискорення.

Запропонований алгоритм формування нового типу S-кривої розгону/гальмування може бути застосований для реалізації “м’якого” прискореного кутового (лінійного) переміщення.

1 И.Ю. Краснов, Е.С. Горюнов. Плавный разгон и торможение промышленных механизмов// Journal of Siberian Federal University. Engineering & Technologies 2 (2014 7), pp. 214-221

2 Han Wu , Jianye Huang, Shuang Lin , Bingqian Liu , Yuanliang Fan , BinyuWu and Zhifan Huang. Application of Improved S-Curve Flexible Acceleration and Deceleration Algorithm in Smart Live Working Robot// Journal of Physics: Conference Series. 2005 012065

3 Zhijie Li , Ligang Cai and Zhifeng Liu. Efficient Planning and Solving Algorithm of S-Shape Acceleration and Deceleration// Wireless Communications and Mobile Computing Volume 2020, Article ID 8884678, 14 pages.

О.А. Владимирський, І.А. Владимирський

ПІДВИЩЕННЯ РЕЗИЛЬЕНТНОСТІ МІСЬКИХ СИСТЕМ ТЕПЛОПОСТАЧАННЯ ШЛЯХОМ ВРАХУВАННЯ ОСОБЛИВОСТЕЙ ЇХ ДІАГНОСТУВАННЯ

Підземні трубопроводи міських теплових мереж України є одними з найбільших серед міських мереж трубопроводів. Високий ступінь загального зносу трубопроводів, що призводить до часто виникаючих витоків, вимагає оперативного та точного їх виявлення. Для споживчів, практично, це означає застосування екскаватора тільки для розриття грунту з метою усунення витоку, а не для його пошуку. Застосування екскаватора в такій якості нерідко вимушено компенсує помилки інструментального течешукання, роблячи пошук тривалим, витратним, не прогнозованим за часом процесом. Така практика знижує резильєнтність системи теплопостачання, її стабільність, стійкість до таких кризових явищ, як витоки. Відійти повністю від цієї практики поки що неможливо через недосконаліть застосовуваних засобів діагностики. Ця недосконаліть проявляється у тому, що розмаїття умов течешукання є ширшим ніж дозволяють можливості застосовуваних методів, методик пошуку витоків і відповідних їм приладів, навіть щодо одного різновиду трубопроводів – теплових мереж. Виробники приладів постійно прагнуть розширити пропоновану номенклатуру. Однак, на звуження області застосування приладів будь-яким одним різновидом трубопроводів і на ускладнення методик застосування відповідних, більш спеціалізованих і при цьому багаторежимних приладів, як правило, відомі виробники йдуть неохоче. Ці підходи, з одного боку, є комерційно невигідними, оскільки звужують ринок збуту, вимагають високої кваліфікації від користувачів, а з іншого боку є дорогими, оскільки вимагають попереднього проведення ретельних досліджень. У цьому є і виклик, і вікно можливостей для вітчизняних розробників.

Серед особливостей теплових мереж, що підлягають врахуванню при пошуку витоків, основними є наступні:

- Присутність на трубопроводах потужних акустичних перешкод від споживачів, зокрема від елеваторів.
- Зношування запірної арматури. Засувки можуть "не тримати", що створює проблеми з відключенням перешкод від споживачів, призводить до виникнення акустичних завад у самих засувках.
- Переважна прокладка труб у непрохідних каналах. Трубопровід не демпфований ґрунтом, що створює умови для складного багатохвильового поширення сигналів витоків, особливо на трубопроводах великого діаметру. Це призводить до неоднозначних показань кореляційних течешукачів.
- Корозійне зношування труб і наявність у них відомих і не відомих вставок від проведених раніше ремонтів. Через це можуть змінюватися

товщина стінки трубопроводу, його діаметр і відповідно швидкість поширення інформаційних акустичних хвиль.

- Дисперсія швидкості інформаційних акустичних хвиль у трубопроводах.
- Залежність показань кореляційних течешукачів від місць встановлення датчиків на трубопровід, інтерференційні спотворення сигналів.
- Відсутність чітких показань приладів через можливе мале відношення сигнал-завада при роботі на протяжних ділянках з безканальною прокладкою з ізоляцією із бітумоперліту, при великих поривах у період гідравлічних випробувань і т.і..

Дослідження механізмів впливу вказаних особливостей на показання течешукачів, проведені в ІПМЕ ім. Г.Є.Пухова НАН України, показали наявність можливостей їхнього врахування за допомогою комплексу заходів. На поточний момент реалізовано наступні:

- Зручний контроль вібрації у теплових камерах та її коректне порівняння у різних місцях для визначення джерел надходячих акустичних сигналів за допомогою течешукача А-10Т3 [1,2].
- Врахування багато хвильового поширення сигналів від витоків та залежність показань кореляційного течешукача від місць встановлення датчиків за допомогою параметричного кореляційного методу пошуку витоків [3,4], який реалізовано у течешукачі К-10.5 різних модифікацій [5].
- Режим параметричного активного методу визначення фактичної швидкості інформативних акустичних хвиль та уточнення координат витоків шляхом додаткового акустичного зондування ділянок трубопроводів з використанням розробленого генератора [6].
- Оснащення течешукача А-10.Т3 чутливим датчиком температури для пошуку витоку не тільки за акустичною, але й за тепловою ознакою у грунті над теплотрасою [1,7].
- Комбінація зазначених режимів для підвищення чутливості та точності визначення витоків при низькому співвідношенні сигнал-завада [7].

Ці та інші режими, методичні прийоми застосування течешукачів розробки ІПМЕ ім. Г.Є.Пухова НАН України, в першу чергу орієнтовані на їхнє використання у теплових мережах. Вони ускладнюють поширену методику пошуку витоків та вимагають відповідної підготовки користувачів. Однак це виправдовується якістю результатів діагностування трубопроводів.

1. А.А.Владимирский, И.А.Владимирский, И.П. Криворучко Термоакустический течеискатель А-10Т3. XXXVIII науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник тез конференції. Київ. 15 травня 2020р. – С 72.
2. Владимирський О.А., Криворучко І.П. Пристрій для установки вібродатчика з магнітним тримачем на ґрунт при пошуку витоків. Патент на корисну модель № 142320; публ. 25.05.2020р., Бюл. №10.

3. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. Електронне моделювання. 2021. 43 (3). С.3-16.
4. Владимирський О.А., Владимирський І.А. Просторовий і частотний кореляційні параметричні методи визначення координат витоків підземних трубопроводів. Електронне моделювання. 2021. 43 (4). С.22-36.
5. О.А. Владимирський, І.А. Владимирський. Параметричний кореляційний течешукач К-10.5М3. Керівництво з експлуатації. К105М3-1.00.04 КЕ. Свідоцтво про реєстрацію авторського права на службовий твір № 110118 від 08.12.2021р. Україна. ІПМЕ ім. Г.Е.Пухова НАН України. –с.31.
6. О.А. Владимирський, І.А. Владимирський. Розробка генератора для акустичного зондування трубопроводів. XLI науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник матеріалів конференції. Київ. 17 травня 2023р.- С 120.
7. О.А. Владимирський, І.А. Владимирський. Визначення координат витоків підземних трубопроводів в умовах малого відношення сигнал-завада. Науково-практична конференція «Кібербезпека енергетики». Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Матеріали. Київ.31 травня 2023р. - С 14.

О.А. Владимирський, І.А. Владимирський

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ АКУСТИЧНОГО ЗОНДУВАННЯ ТРУБОПРОВІДІВ ПРИ ПОШУКУ ВИТОКІВ ДЛЯ ПІДВИЩЕННЯ РЕЗИЛЬЄННОСТІ ТЕПЛОПОСТАЧАННЯ

При пошуку витоків у підземних напірних трубопроводах найбільше розповсюдження набули акустичні пасивні методи, засновані на реєстрації акустичного шуму, створюваного в місці пошкодження витоком середовища, що транспортується. Застосування ж активних методів для пошуку витоків знаходить набагато менше практичне застосування. Разом з тим, інтерес до них у публікаціях є високим. Здебільшого цей інтерес викликаний прагненням діагностувати протяжні ділянки підземних трубопроводів шляхом створення ударної хвилі у транспортованому середовищі та реєстрації відлунь від місць локального зниження тиску в області витоку [1,2,3]. Для формування хвилі використовуються спеціальні керовані клапани. Методи будуються на різноманітних алгоритмах обробки перехідних процесів, що відбуваються у трубопроводі в області формування хвилі тиску.

Також на основі відбиттів, але ж для акустичних хвиль у стінці трубопроводу, застосовуються ультразвукові прилади Wavemaker [4,5]. Використовуються поздовжні та крутильні хвилі, що формуються п'єзоелектричними або, у інших приладах, магнітострикційними віброперетворювачами, закріпленими на підготовленій поверхні трубопроводу. Дані прилади призначені для дистанційного визначення місць та оцінки ступеня потонання металу у вигляді середньої за площою перерізу стінки втрати металу трубопроводу. Відповіді на запитання, чи є наскрізне пошкодження у виявленому місці або його там ще немає, прилади не дають.

Іншим застосуванням зондування трубопроводів є визначення характеристик поширення по ньому акустичних хвиль. Таких характеристик, як фазова та групова швидкість, коефіцієнт загасання. Ці характеристики, зокрема, використовуються для калібрування пасивних ультразвукових акустоемісійних засобів діагностики трубопроводів. Застосування зондування трубопроводів для уточнення швидкості хвиль при пошуку витоків представлено в ряді патентів, наприклад у [6]. Однак, широкого практичного застосування цього напрямку не виявлено. Разом з тим, для діагностики підземних трубопроводів України цей напрямок є актуальним з наступних причин:

- В одному з двох найбільш інтенсивно застосовуваних типів течешукачів – кореляційних, вихідним параметром визначення координати витоку є швидкість хвиль гідравлічного удару. Ця швидкість вибирається з запрограмованих у приладах розрахункових значень для конкретного діаметра трубопроводу. Однак, швидкість також залежить і від товщини

стінки трубопроводу, через що, в умовах її корозійного потонання, вона може відрізнятися до 30% і більше.

- Підземні трубопроводи, як циліндричні оболонки та шаруваті середовища, мають властивість багатохвильового та дисперсійного поширення по них акустичних хвиль. Широке розмаїття наявних умов і типів прокладки трубопроводів, замуленість непрохідних каналів, широке застосування трубопроводів з великими, порівняними з довжинами інформаційний хвиль діаметрами, призводить і до широкого розмаїття швидкостей домінуючих за потужністю акустичних хвиль, властивих різним ділянкам трубопроводів з однаковими діаметрами.

Врахування зазначених особливостей дозволило б значно підвищити точність визначення місць витоків і, як наслідок, оперативність їх усунення, що є важливим для забезпечення задовільної резильєнтності системи теплопостачання. З метою практичного відпрацювання цього напряму на базі течешукача К-10.5, розробленого в ІПМЕ ім. Г.Є.Пухова НАН України, додатково створені акустичний випромінювач та генератор [7].

1. Niloufar Motazedi and Stephen Beck. Leak detection using cepstrum of cross-correlation of transient pressure wave signals. Mechanical Engineering Science 2018, Vol. 232(15) 2723–2735. DOI: 10.1177/0954406217722805.
2. Adel Belouchrani, Moeness G. Amin, Nadıge Thirion-Moreau, and Yimin D. Zhang. Source Separation and localization using time-friquency distributions. IEEE Signal Process Mag 30 (6): 97–107 IEEE.
3. Lee P.J., Vítkovský J.P., Lambert M.F., Simpson, A.R. and Liggett, J.A. Leak location in pipelines using the impulse response function. Journal of Hydraulic Research 45(5):643-652. DOI:10.1080/00221686.2007.9521800.
4. *Peter Cawley* Practical long range guided wave inspection - applications to pipes and rail Department of Mechanical Engineering, Imperial College, London SW7 2BX, UK NDE2002 predict. assure. improve. National Se minar of ISNT Chennai, 5. – 7. 12. 2002. Режим доступу:http://citeseerx.ist.psu.edu/viewdoc/download? doi= 10.1.1.471.787&rep= rep1&type=pdf.
5. Wavemaker-g4: Guided Ultrasonics Ltd (GUL) Products Overview, available at: https://www.guided-ultrasonics.com/wavemaker-g4/.
6. Патент KR20160110722A 2016-09-22 HYDRONET CO LTD [KP]. Earliest priority: 2015-03-11 Earliest publication: 2016-09-22 Inventors PARK JUNE KEE [KR]; KWON SUNG WON [KR].
7. О.А. Владимирський, І.А. Владимирський. Розробка генератора для акустичного зондування трубопроводів. XLI науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник матеріалів конференції. Київ. 17 травня 2023р.- С 120.

П.П. Лобода

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО ДВІЙНИКА ДЛЯ ПІДГОТОВКИ ПЕРСОНАЛУ НОВОГО БЕЗПЕЧНОГО КОНФАЙНМЕНТУ ЧАЕС

Серед критичної інфраструктури України особливе місце займає Чорнобильська атомна електростанція (ЧАЕС) та Новий безпечний конфайнмент (НБК), який був побудований за допомоги світової спільноти для захисту населення та довкілля від розповсюдження радіоактивного забруднення з побудованого ще у 1986 році об'єкта «Укриття», термін експлуатації якого вже закінчився.

НБК являє собою складний технічний об'єкт, який представлено ізоляційною арочною спорудою великих розмірів, обладнану різноманітними системами моніторингу та управління. До основних проблем функціонування НБК можна віднести вплив підвищеного радіаційного фону в основному об'ємі споруди на виробничий персонал та неконтрольовані витоки радіаційного забруднення за її межі. Стіни та дах старого об'єкту «Укриття» в наслідок його поступового руйнування мають достатньо велику кількість щілин, через які повітря разом з радіоактивними аерозолями проникають в основний об'єм НБК, а потім в оточуюче середовище. Перепади температур усередині НБК, вітрове навантаження на конструкції НБК викликають певні нестаціонарні процеси теплової конвекції та руху повітря [1]. Належна експлуатація систем НБК є необхідною умовою забезпечення захисту довкілля та гарантування його тривалого використання, для чого необхідно підтримувати високий рівень підготовки виробничого персоналу. Враховуючи, що плановий термін експлуатації НБК становить 100 років, організація ефективного процесу підготовки його виробничого персоналу є актуальною задачею, для вирішення якої можна використовувати цифрові двійники.

У загальному розумінні цифровим двійником називають віртуальний прототип реального фізичного об'єкту, виробу, групи виробів чи процесу, який виконує збір та повторне використання цифрової інформації. Цифровий двійник, здебільшого, складається з двох частин: комп'ютерної візуальної моделі об'єкта та поведінкової моделі, що містить відповідні математичні моделі та моделі даних. За своїм призначенням цифрові двійники поділяються на цифрові двійники-прототипи, цифрові двійники-екземпляри та цифрові двійники-агрегати, що поєднують кілька цифрових двійників-екземплярів [2]. За типом зв'язку між цифровим двійником і реальним об'єктом їх можна поділити на цифрові моделі (автоматизований обмін даними відсутній), цифрові тіні (двійник тільки отримує дані з об'єкту) та, власне, цифрові двійники (присутній двонаправлений обмін даними між двійником та об'єктом) [3].

Цифровий двійник НБК може бути використаний для візуалізації інформації стосовно його поточного стану, підтримки прийняття рішень щодо керування його підсистемами та навчання персоналу шляхом, наприклад, моделювання процесів управління. Відповідні функції реалізуються у програмному забезпеченні цифрового двійника НБК, узагальнена діаграма прецедентів якого представлена на рисунку 1.

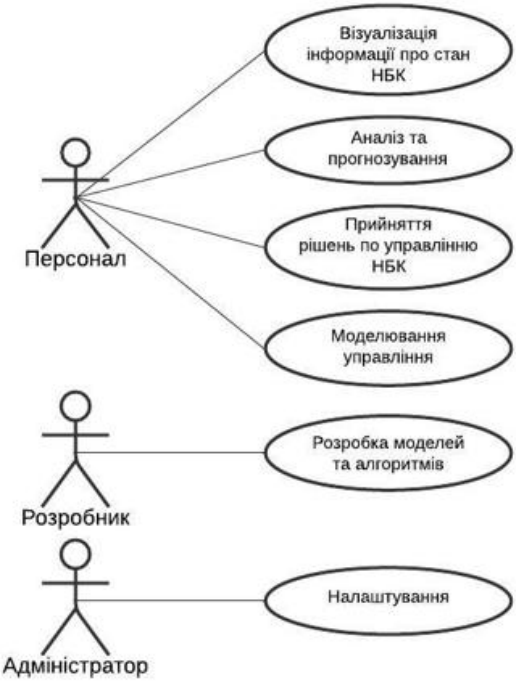


Рисунок 1 – Узагальнена діаграма прецедентрів цифрового двійника НБК

Застосування цифрового двійника НБК дозволить реалізувати у навчанні його персоналу моделювання реальних виробничих ситуацій, пов'язаних з управлінням та прийняттям рішень.

1. Круковский П.Г., Метель М.А., &Скляренко Д.И. (2019) *Новый безопасный конфайнмент Чернобыльской АЭС (расчетно-экспериментальный анализ при* проектировании и эксплуатации). ООО "Франко Пак".
2. Grieves M. (2019) Virtually Intelligent Product Systems: Digital and Physical Twins. Complex Systems Engineering: Theory and Practice. *American Institute of Aeronautics and Astronautics*, 175-200. DOI :10.2514/5.9781624105654.0175.0200.
3. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W. (2018) Digital Twin in manufacturing: a categorical literature review and classification. *IFACPapersOnLine*, 51 (11), 1016–1022. https://doi.org/10.1016/J.IFACOL.2018.08.474.

С.С. Шевченко

ІНТЕРАКТИВНІ АВТОМАТИЗОВАНІ ДИСТАНЦІЙНІ НАВЧАЛЬНО-ТРЕНУВАЛЬНІ СИСТЕМИ ЯК ВАЖЛИВА ЛАНКА У РЕЗИЛЬЄНТНОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Надійна та безперебійна робота об'єктів критичної інфраструктури залежить від підготовки та підтримання на належному рівні кваліфікації персоналу. За рахунок правильної експлуатації обладнання можна підвищити безпеку та надійність роботи об’єктів, подовжити термін експлуатації, підвищити енергоефективність механізмів та систем за рахунок вибору правильного режиму роботи, а також своєчасно та коректно реагувати на нестандартні виклики. Все це вимагає високого рівня кваліфікації спеціалістів з обслуговування.

Також дуже важливо мати необхідну інформацію у максимально наглядному вигляді та найшвидшому доступі. У сенсі резильєнтності це не тільки навчання персоналу з метою довгострокової передачі знань, але й можливість ці знання отримати дуже швидко в критичних умовах.

Повна картина передачі знань дає два виміри передачі знань: ефективність та результативність. Ефективність визначається як швидкість, з якою одержувач отримує нові знання [1]. Результативність розуміється як рівень засвоєння знань суб'єктом-одержувачем [2].

Найбільш ефективними та результативними за сумою всіх факторів вважаються комп’ютерні тренажери та системи навчання, що використовують новітні інформаційні технології [3], одною з важливих рис яких є спроможність забезпечити швидке якісне навчання та підготовку персоналу, в тому числі і в дистанційному, а також індивідуальному режимі. Інтерактивність та наочність забезпечують найвищий рівень інтеграції знань у пам’ять та навички користувача, а можливість програвати певні сценарії у процесі навчання дозволяють здобувати знання на прикладі різноманітних ситуацій, що практично повністю емулює отримання знань шляхом життєвого досвіду, тільки без ризиків та за значно більш короткий проміжок часу.

Створення інтерактивних навчальних матеріалів з використанням 3D-технологій (рис.1) дозволить максимально стисло та ефективно передавати досвід та знання спеціалістам, а використання сучасних веб-технологій дозволяє знизити вартість та час навчання за рахунок зниження вартості обладнання, необхідного для проведення навчання, а також за рахунок проведення дистанційного та автоматизованого навчання. Також інтерактивні навчальні матеріали можуть бути використані як посібники у разі нештатних ситуацій з метою надання необхідних знань залученим у ліквідацію проблеми людям.

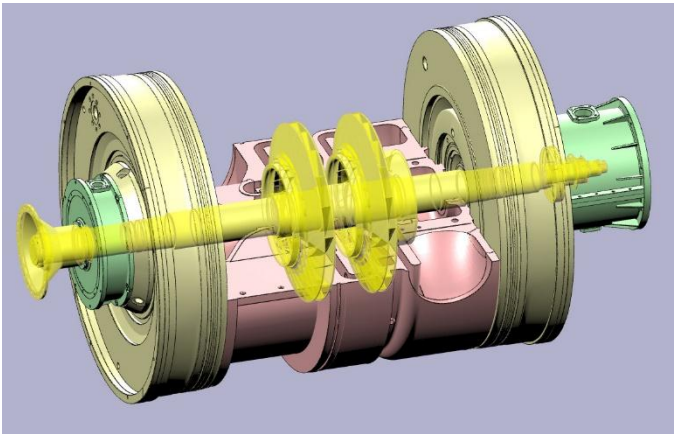


Рисунок 1 – Приклад роботи інтерактивної системи на базі 3D-технологій

Підвищення ефективності навчання та контролю за навчальним процесом дозволить покращити якість підготовки обслуговуючого персоналу, за рахунок чого знизиться ймовірність аварій. А у разі настання нештатних ситуацій буде можливість своєчасно забезпечити інформацією для якісного реагування. Все це дозволить тримати резильєнтність об'єктів інфраструктури на достатньо високому рівні.

1. P´erez-Nordtvedt, L., Kedia, B. L., Datta, D. K., and Rasheed, A. A. (2008). Effectiveness and efficiency of cross-border knowledge transfer: an empirical examination. Journal of Management Studies, 45(4):714–744.
2. Jensen, R. J. and Szulanski, G. (2007). Template use and the effectiveness of knowledge transfer. Management Science, 53(11):1716–1730.
3. Nikos Andriotis (2018). Five popular employee training methods for workplace training. eLearning Industry, https://elearningindustry.com/how-choose-training-methods-for-employees

В.Ю. Зубок, Р.С. Драгунцов

ПРОЄКЦІЯ ПРИНЦИПІВ НАЦІОНАЛЬНОЇ СИСТЕМИ СТІЙКОСТІ ТА РЕЗИЛЬЄНТНІСТЬ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Законодавство України визначає об'єкти критичної інформаційної інфраструктури (ОКІІ) як інформаційні технології (ІТ) та операційні технології (ОТ), які є невід'ємними частинами об'єктів критичної інфраструктури (ОКІ) [1]. ОТ працюють у складі кіберфізичних систем, кінцевим продуктом яких є матеріальний об'єкт, в той час як кінцевим продуктом ІТ є інформація. Однак цифрова трансформація призводить до конвергенції цих технологій. Цифрова трансформація (або, як її називають в ЗМІ, «цифровізація» чи «діджиталізація») - характерна риса цифрового суспільства, економіка якого базується на інформаційних технологіях. Семантичне поле цифрової трансформації включає в себе такі поняття, як цифрова економіка, цифрові навички, цифрові права, цифрові інновації, електронні послуги, електронне урядування і багато іншого. Через це в ареал критичної інфраструктури вже потрапляють об'єкти, що мають важливе значення у сферах електронних комунікацій [2]. В новій директиві ЕС, відомій під назвою NIS2 [3] визначено нові підходи кіберрезильєнтності: визначено певні сектори цифрових послуг - онлайн-ринки, онлайн-пошукові системи та служби хмарних обчислень, в яких суб'єкти, що надають значну долю послуг на ринку, потрапляють під контроль з боку державних органів, відповідальних за кібербезпеку.

Викладене свідчить, що до ОКІІ на рівні з традиційними секторами критичної інфраструктури де факто потрапляють не тільки інфокомунікаційні системи підприємств, що постачають життєво важливу продукцію та послуги, а й різні види електронних комунікації, центри обробки даних, інші фізичні та віртуальні ІТ-інфраструктури.

Відповідно до [4], національна система стійкості (надалі – НСС) призначена для забезпечення здатності держави і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики національній безпеці, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко і повномасштабно відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, зокрема гібридних.

Одним з найперших базових елементів, функціонування яких має забезпечити НСС, є безпека та захищеність об'єктів критичної інфраструктури. В основу НСС покладено одинадцять принципів. Серед них, зокрема, присутні:

- готовність;
- мобільність;
- адаптивність;

– наявність резервів;
– безперервність.

Перелічені принципи значною мірою утотожнюють поняття стійкості із поняттям резильєнтності. На сьогодні добре відомі поняття кіберстійкості (cyber resilience) [5] та цифрової стійкості (digital resilience) [6]. Є різні підходи до тлумачення різниці між ними. Аналіз джерел дозволяє зробити висновок, що обидва мають відношення до управління безперервністю бізнесу (business continuity management, або BCM). Втім, сфера застосування поняття кіберрезильєнтності ставить в середину концепції стійкість та відновлюваність інфокомунікаційних систем до кіберзагроз, в той час як цифрова резильєнтність – це більше про властивості та поведінку окремого індивіда, групи чи спільноти під впливом тих самих кіберзагроз [7].

З цифрової резильєнтності додатково ще виокремлюють поняття *цифрової операційної резильєнтності* (digital operations resilience), описаної в DORA [8]. Цифрова операційна резильєнтність фокусується на спроможності ІКТ-ресурсів організації забезпечити BCM у випадку кризових подій.

Розглянемо згадані чотири принципи, закладені в основу НСС, в проєкції на *цифрову операційну резильєнтність* ОКІІ.

Готовність передбачає наявність планів дій щодо спільного реагування на будь-які загрози, належний рівень теоретичної і практичної підготовки усіх суб'єктів забезпечення національної стійкості до реагування на загрози і кризові ситуації на усіх етапах циклу забезпечення національної стійкості;

Мобільність означає здатність до швидкого залучення основних і резервних сил, засобів, ресурсів та об'єднання зусиль для вирішення завдань в умовах виникнення загрози, настання кризової ситуації;

Адаптивність – це здатність системи пристосовуватися до кризових умов і нових обставин, які виникли під впливом загрози або кризової ситуації, забезпечувати виживання, еволюцію, можливість трансформувати негативні результати в позитивні, а також застосовувати інноваційні рішення;

Наявність резервів вимагає присутності у системі додаткових спроможностей, які можуть бути задіяні внаслідок виходу з ладу основних, а також альтернативних планів, стратегій розвитку;

Безперервність – це продовження діяльності системи та усіх суб'єктів забезпечення національної стійкості без значної втрати функціональності.

Ще один принцип, закладений в основу НСС, а саме – *субсидіарність*, передбачає такий розподіл повноважень і відповідальності, при якому ключові рішення щодо реагування на загрози і кризові ситуації ухвалюються на найнижчому можливому рівні. Це дає право стверджувати, що резильєнтність має починатись з найнижчої ланки – безпосередньо користувача цифрових послуг. Саме на цьому рівні ухвалюються рішення з пом'ягшення ризиків для цифрової екосистеми шляхом застосування елементів та методів, що знаходяться в зоні відповідальності користувача. Приклади таких заходів з цифрової операційної резильєнтності на рівні кінцевого споживача проаналізовано в [9].

В державі, енергосистема якої піддається цілеспрямованим атакам та має суттєві пошкодження, для будь-якої ІКС утворюється певна сукупність загроз, до таких можна віднести:

– планові (стабілізаційні) відключення електропостачання на об’єктах ІКС, що обмежують час функціонування систем;

– аварійні та екстренні відключення електропостачання на об’єктах ІКС, що призводять до неочікваних збоїв та відмов;

– аварійні параметри електричній мережі (відхилення напруги) які фізично загрожують обладнанню ІКС.

Дані загрози можуть створювати певну кількість ризиків для функціонування системи [10]. Переважна частина політик безпеки, що застосовуються в ІКС, передбачають можливість відсутності електропостачання протягом певного періоду часу та передбачають відповідні контрзаходи на випадок таких ситуацій [11]. Однак дані розрахунки найчастіше не беруть до уваги ситуацію з систематичним руйнуванням зовнішніх енергосистем. тому пропонується розглянути чотири основні заходи резильєнтності, які здатні системно вплинути на перебіг кризи в ІКС підчас аварій мереж електропостачання (Табл.1)

Таблиця 1 – Огляд заходів з резильєнтності

Захід	Переваги	Недоліки
Резервне живлення від акумуляторних батарей батарей (ДБЖ)	Забезпечення функціонування об’єкту в умовах відключення електропостачання; Можливість моніторингу стану батареї, що зменшує ризики щодо спостережності.	Час підтримки функціонування об’єкту відносно нетривалий; Батареї великої ємності потребують або тривалого часу заряджання, або спеціальних зарядних пристроїв; несуть додаткову небезпеку.
Резервні генератори	Забезпечення функціонування об’єкту в умовах відключення електропостачання протягом потенційно необмеженого часу; Можливість резервування порівняльно більшої електричної потужності.	Створює логістичне та організаційне навантаження на підтримку функціонування; ускладнений централізований моніторинг стану генераторів, регулярне технічне обслуговування.

Географічне розподілення	Можливість нівелювати ризики відключень по відношенню до однотипних компонентів системи; У разі міждержавного розподілу дозволяє забезпечити гарантований захист частини ІКС.	Для багатьох ОКІ неможливо географічне розподілення чи перенесення. Не вирішує проблему відключення унікальних компонентів ІКС; Не забезпечує захисту від блекаутів (екстрених вимкнень всієї мережі). Існують окремі категорії ІКС, які не дозволено винести в безпечну зону (за межі держави).
Перенесення в хмару	Гарантований захист від відключень електропостачання винесених компонентів.	Неможливо перенести усі компоненти ІКС в хмару, особливо це стосується операційних технологій та ОКІІ. Вимоги Tier III до ЦОД вимагають лише 72 години автономної роботи.

Враховуючи вище викладені міркування, можемо дійти висновку щодо можливих підходів до моделювання загроз пов’язаних з масштабними відключеннями електропостачання. Щоб врахувати цей фактор, можна використовувати наступні підходи:

1. Моделювання відключення електропостачання як окремої загрози: можна включити в модель загрозу відключення електропостачання як окрему загрозу, з оцінкою ймовірності та відповідними наслідками.

2. Врахування взаємозв'язку між електропостачанням та функціонуванням інших системами: можна включити в модель взаємозв'язки між електропостачанням та іншими критичними системами, такими як мережі електрозв'язку, банківські системи, системи зберігання даних. Це дозволить оцінити, як відключення електропостачання може вплинути на роботу цих систем та які наслідки можуть мати.

3. Моделювання відновлення електропостачання: можна включити в модель процес відновлення електропостачання після відключення, з оцінкою тривалості та наслідків цього процесу. Це дозволить оцінити, як довго може зайняти відновлення електропостачання та як це може вплинути на інші системи, зокрема таких, що належать до засобів забезпечення кібербезпеки.

4. Використання симуляційного моделювання: пропонується використовувати симуляційне моделювання, щоб оцінити, як відключення

електропостачання може вплинути на роботу інших систем та якими можуть бути наслідки, зокрема для кібербезпеки.

1. Деякі питання об’єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943 : станом на 07.09.2022р. URL : https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF (дата звернення: 09.02.2023)
2. Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв`язку. Рішення від 24 травня 2023 року №210. URL : https://nkrzi.gov.ua/index.php?r=site/index&pg=533&id=10603&language=uk
3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.
4. Концепції забезпечення національної системи стійкості. Затверджено Указом Президента України від 27 вересня 2021 року № 479/2021. URL : https://zakon.rada.gov.ua/laws/show/479/2021/print
5. Linkov, I., Kott, A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Kott, A., Linkov, I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. https://doi.org/10.1007/978-3-319-77492-3
6. Cuel, R., Ponte, D., & Virili, F. (2022). Exploring digital resilience: Challenges for people and organizations. Springer Nature.
7. UK Council on Internet Safety. Digital Resilience Framework : станом на 18.09.2020. URL : https://www.gov.uk/government/publications/digital-resilience-framework
8. Digital Operational Resilience Act (Regulation (EU) 2022/2554). URL: https://www.digital-operational-resilience-act.com/
9. В. Зубок. Ефективність використання заходів з підвищення цифрової стійкості підчас тривалих відключень електропостачання // Електронне моделювання. - 2023 - 45(1). – с.98-112. – DOI:10.15407/emodel.45.10.098
10. What happens during a blackout / T. Petermann et al. Norderstedt : BoD – Books on Demand, 2011
11. Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). STRIDE-based threat modeling for cyber-physical systems. У 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE. https://doi.org/10.1109/isgteurope.2017.8260283

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«РЕЗИЛЬЄНТНІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ – 2023»

Збірник матеріалів конференції

21 червня 2023 р.

Critical Infrastructure Resilience – 2023 : collection of materials of the scientific and practical conference, Kyiv, June 21, 2023, PIMEE of NAS of Ukraine. - 2023. - 109 p.

Резильєнтність критичної інфраструктури – 2023 : збірник матеріалів науково-практичної конференції, м. Київ, 21 червня 2023 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2023. – 109 с.