UDK 004.8:005.52:004.9

Olga Degtiareva[12]
Tetiana Kuklinova[3]
Valeriia Slatvinska[3]
Volodymyr Hura[3]
Oleksandr Zadereiko[3]

MODERN CONTEXT OF DIGITAL RESILIENCE AND RISK MANAGEMENT IN AI-RELATED INNOVATION PROJECTS

Absract. *Digital resilience is essential for maintaining the secure and continuous operation of modern energy infrastructure amid growing cyber- and hybrid-threats. The integration of artificial intelligence (AI) enhances situational awareness, predictive monitoring, and adaptive decision-making, mitigating operational risks and supporting service continuity. At the same time, intelligent systems introduce new vulnerabilities, necessitating structured risk management and resilience-focused governance. Drawing on Ukraine's experience, including cyber incident trends and sector-specific vulnerabilities, this study highlights the effectiveness of combining technological, organizational, and managerial measures to sustain energy operations. Standardized resilience metrics, AI-driven risk mitigation, and regional collaboration are critical for securing interconnected energy networks. The findings provide guidance for operationalizing digital resilience in energy-related projects.*

Key words. *Innovations; AI; Digital Resilience; Energy Infrastructure; Risk Management; Energy Management, Organizational Management; Hybrid Threats.*

[1] University of Applied Sciences Mittweida, Technikumplatz 1, 09648 Mittweida, Germany

[2] Odesa National Economic University, Preobrazhenska 8, 65082 Odesa, Ukraine

[3] National University «Odesa Law Academy», Fontanska Doroga 23, 65009 Odesa, Ukraine

AI-related innovation projects have often been perceived as sources of organizational vulnerability and complexity. However, recent research increasingly emphasizes their potential to enhance the resilience of organizations and society [1]. This perspective is reflected in the concept of *digital resilience*. Resilience broadly refers to a system's capacity to absorb, adapt to, and recover from disruptions, while digital resilience stresses the role of information systems in enabling and strengthening these capabilities in digitally mediated environments. In parallel, the digital transformation of critical infrastructures is reshaping approaches to their management, particularly in the context of energy systems. Within this domain, digital resilience refers to the ability of systems to maintain continuous operation despite disruptions, cyberattacks, or crisis events. Achieving such resilience increasingly relies on the integration of advanced analytical and automation technologies, most notably artificial intelligence (AI), which enables improved monitoring, decision-making, and adaptive system responses. AI-driven tools enhance situational awareness, enable predictive monitoring, and support adaptive decision-making and adaptive system responses in complex environments. At the same time, the growing reliance on intelligent systems introduces new categories of operational and cyber risk, requiring structured risk management frameworks. Effective governance therefore demands the alignment of AI capabilities with comprehensive risk assessment, mitigation strategies, and resilience-oriented system design to ensure the secure and stable functioning of critical energy infrastructure.

2024 was characterized by a significant increase in cyber threats. 4,315 cyber incidents were recorded. This is 70% more than in 2023 (2,541 cases) [1]. Local authorities are most often attacked (34%). The security and defense sector is a significant target (23%). Next are state institutions (19%). Energy and telecommunications remain vulnerable. Phishing dominates among attack methods (27%). The use of malicious software is widespread (21%). Account compromise is also recorded (5.4%). Despite the overall increase in the number of incidents, critical consequences remain rare. In 2024, only four incidents with critical impact were recorded. The Ukrainian cybersecurity market was worth $138 million in 2024. The market has grown fourfold in the past eight years, driven primarily by the need to address growing threats [3]. In 2024, the energy sector experienced a total of 251 cyberattacks, highlighting its vulnerability within critical infrastructure systems [4].

The combination of cybersecurity, modern technologies and management solutions helps maintain system stability [5]. Modern energy infrastructure is becoming increasingly interconnected and reliant on digital and information technologies, which, while improving operational efficiency, simultaneously introduce new cyber vulnerabilities. Cybersecurity emerges as a critical component of energy system protection. Ensuring the reliability and continuity of energy supply therefore requires not only technical safeguards but also a broader framework of digital resilience. Such resilience enables energy networks to anticipate, withstand, adapt to, and rapidly recover from cyber disruptions, thereby supporting the stable functioning of critical infrastructure.

Ukraine's experience shows that digital resilience is a necessary condition for the functioning of the energy sector during hybrid threats. This is especially important for the energy sector, as the stability of energy supply contributes to national security and economic stability.

Cyber risks in contemporary energy infrastructure can be structured into operational technology (OT), systemic, and service-availability threat domains. OT-focused risks include targeted intrusions into SCADA/ICS environments, exploitation of unpatched legacy platforms, ransomware deployment, and falsification of sensor or telemetry data, all of which threaten real-time process integrity and control reliability. Systemic and availability threats—such as insider compromise, supply chain infiltration, phishing-driven credential abuse, IoT exploitation, and DDoS campaigns—degrade data trustworthiness, coordination mechanisms, and network continuity, reinforcing the necessity for integrated digital resilience architectures and formal risk management frameworks.

Cyberattacks targeting Ukraine’s energy infrastructure may produce cascading effects that extend beyond national boundaries, potentially affecting interconnected or technologically comparable energy systems in neighboring countries. The architectural similarities of grid topologies, legacy control systems, and equipment configurations common across many regional networks increase the likelihood that exploit techniques can be replicated. This cross-system vulnerability underscores the need for digital resilience frameworks capable of mitigating systemic cyber risks, enabling coordinated detection, response, and recovery mechanisms. Strengthening resilience at both national and regional levels is therefore essential to limit propagation effects and preserve the operational stability of interconnected energy infrastructures.

AI and ML enable advanced predictive analytics, real-time monitoring, and adaptive control of complex processes, allowing operators to optimize energy generation, distribution, and consumption. These technologies support automated fault detection, anomaly identification, and dynamic load balancing, reducing downtime and operational risks. Moreover, AI-driven decision support systems facilitate data-informed planning and resource allocation, contributing to long-term system resilience. Integrating AI and ML with cybersecurity and risk management frameworks further ensures the secure, stable, and continuous operation of critical energy infrastructure under evolving threats. The coordinated deployment of heterogeneous AI modalities enables a multi-layered cybersecurity architecture for power plant environments. Analytical, functional, interactive, textual, and visual AI components collectively enhance anomaly detection, automated response orchestration, operator decision support, and situational awareness, thereby reducing operational risk and supporting the continuity of critical energy processes [1]. The effectiveness of such AI-driven protection depends on the parallel integration of managerial innovations—including adaptive governance models, risk-based decision frameworks, and resilience-oriented operational policies—which align intelligent automation with organizational cyber defense strategies to strengthen the protection of energy infrastructure.

The effective management of digital resilience within energy enterprises requires the integration of technical, organizational, and strategic measures. Governance structures should define clear roles and responsibilities for cybersecurity, operational continuity, and incident response across all organizational levels. Continuous monitoring, real-time threat detection, and predictive analytics must be complemented by regular risk assessments and scenario-based simulations to ensure system robustness. Employee training, awareness programs, and adaptive operational policies are essential to mitigate human-factor vulnerabilities and enhance organizational preparedness. Furthermore, the alignment of intelligent automation tools, such as AI-driven anomaly detection, with formal risk management frameworks fosters a proactive and coordinated approach to sustaining uninterrupted energy operations.

Therefore, digital resilience is essential for ensuring the secure and continuous operation of modern energy infrastructure amid escalating cyber- and hybrid-threats. The integration of AI enhances situational awareness, predictive monitoring, and adaptive decision -making, mitigating operational risks and supporting service continuity. At the same time, intelligent systems introduce new vulnerabilities, requiring structured risk management and resilience-focused governance. Ukraine's experience demonstrates that combining technological, organizational, and managerial measures can sustain energy operations under adverse conditions. Advancing standardized resilience metrics, AI-driven mitigation strategies, and regional cooperation is critical for securing interconnected energy networks globally.

REFERENCES

1. Degtiareva O., Shyriaieva N. Kuklinova T. Artificial Intelligence Solutions for Cybersecurity in Energy Systems. *2024 IEEE International Workshop on Technologies for Defense and Security.* Naples, Italy. 2024, pp. 177-182.

2. CERT-UA processed 4,315 cyber incidents last year*. State Service of Special Communications and Information Protection of Ukraine.* 2025. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (accessed Jan. 23, 2026).

3. IT Ukraine Association, *Overview of the Cybersecurity Market in Ukraine*, DataDriven Research & Consulting, IT Ukraine Association, Kyiv, Ukraine, 2025. URL: https://itukraine.org.ua/files/Ukraine Cybersec Market Review.pdf (accessed Jan. 23, 2026).

4. Russian cyber operations: analytics for the H2 2024. *State Service of Special Communications and Information Protection of Ukraine. Kyiv: State Service of Special Communications and Information Protection of Ukraine,* 2024. 22 p.

5. Horbachenko S. The Role of Cybersecurity Management in Contemporary Management Science and Practice. *Sustainable Economic Development*, 2024 vol. 1, no. 48, pp. 144–149. URL: https://doi.org/10.32782/2308-1988/2024-48-19

Degtiareva Olga O., *Doctor of Economic Sciences, Professor at the Institute of Energy Management, University of Applied Sciences, Mittweida, Germany, email: degtiare@hs-mittweida.de & Odesa National Economic University, Odesa, Ukraine.*

Kuklinova Tetiana V., *PhD in Business Administration, Associate Professor of the Department of Artificial Intelligence and Mathematical Modeling, National University «Odesa Law Academy», Odesa, Ukraine.*

Slatvinska Valeriia M., *PhD in Law, Lecturer of the Department of Cybersecurity, National University «Odesa Law Academy», Odesa, Ukraine.*

Hura Volodymyr I., *PhD in Computer Science, Associate Professor of the Department of Artificial Intelligence and Mathematical Modeling,National University «Odesa Law Academy», Odesa, Ukraine.*

Zadereiko Oleksandr V., *PhD in Computer Science, Associate Professor of the Department of Artificial Intelligence and Mathematical Modeling, National University «Odesa Law Academy», Odesa, Ukraine.*