INNOVATION AND SUSTAINABILITY
Volume 6, No. 2. 2026
ISSN 2786-5940, e-ISSN 2786-5959
Received: 19.11.2026; Revised: 30.04.2026;
Accepted: 25.06.2026; Published: 10.07.2026
Journal homepage: https://inns.com.ua/en

UDC 004.8:005.52:004.9
DOI: 10.31649/vis/2.2026.34

Risk-oriented product management of AI-based solutions in the energy sector

Olga Degtiareva
Doctor of Economic Sciences, Professor
University of Applied Sciences Mittweida
09648, 1 Technikumplatz, Mittweida, Germany
Odesa National Economic University
65000, 8 Preobrazhenska Str., Odesa, Ukraine
https://orcid.org/0000-0003-1276-334X

Tetiana Kuklinova*
PhD in Economic Sciences, Associate Professor
National University "Odesa Law Academy"
65009, 23 Fontanska Doroha Str., Odesa, Ukraine
https://orcid.org/0000-0002-1370-2883

Valeriia Slatvinska
PhD in Law, Lecturer
National University "Odesa Law Academy"
65009, 23 Fontanska Doroha Str., Odesa, Ukraine
https://orcid.org/0000-0002-6082-981X

Volodymyr Hura
PhD in Technical Sciences, Associate Professor
National University "Odesa Law Academy"
65009, 23 Fontanska Doroha Str., Odesa, Ukraine
https://orcid.org/0000-0001-6415-7865

Oleksandr Zadereiko
PhD in Technical Sciences, Associate Professor
National University "Odesa Law Academy"
65009, 23 Fontanska Doroha Str., Odesa, Ukraine
https://orcid.org/0000-0003-0497-9861

Abstract. AI-related innovation initiatives in the energy sector have traditionally been viewed as sources of organisational complexity and potential vulnerability. The study aimed to analyse the interplay between energy security and the resilience of energy systems, to explore emerging risks associated with digitalisation and the implementation of intelligent systems, and to evaluate the managerial and policy measures necessary for the effective integration of AI into energy infrastructure. To achieve the stated objectives, open-access sources were utilised and an integrated approach was applied, combining general scientific and specialised research methods, with particular emphasis on advanced analytical, monitoring and automated technologies. The findings underscored the importance of investing in technological, human, and regulatory capacities to fully leverage the potential of AI. At the same time, the role of AI-driven tools in modern energy systems is increasing due to their contributions to digital resilience, operational stability, predictive maintenance, cybersecurity, and strategic decision-making. However, these developments are accompanied by corresponding risks. That is why the modern management system must evolve from an administrative and control-oriented function to an

Suggested Citation:
Degtiareva, O., Kuklinova, T., Slatvinska, V., Hura, V., & Zadereiko, O. (2026). Risk-oriented product management of AI-based solutions in the energy sector. *Innovation and Sustainability*, 6(2), 34-45. doi: 10.31649/vis/2.2026.34.

*Corresponding author (*tanya2013001@gmail.com*)

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

intelligent, analytical mechanism that integrates human expertise with algorithmic decision-making. In this way, digital resilience extends the concept of system resilience by integrating information technologies and AI-driven analytics to anticipate, absorb, and recover from disruptions, whether caused by physical, technological, or cyber incidents. This integration reduces subjectivity, enhances the accuracy of operational decisions, and ensures a transparent, adaptive, and scientifically grounded approach to strategic coordination. By combining advanced analytics, AI-driven automation, and proactive risk management, energy systems can achieve enhanced stability, operational reliability, and cybersecurity resilience in increasingly complex and digitally interconnected environments. Furthermore, leveraging global best practices and fostering cross-border collaboration in AI innovation and cybersecurity can accelerate the transformation of energy enterprises toward sustainable, intelligent, and resilient infrastructures

Keywords: digital environment; cyber risks; investments; product management; strategic planning; project management; operational risk

Introduction

The growing number of AI-related innovation projects and the increasing role of AI-driven tools in modern energy systems are accompanied by newly emerging operational risks, including cyberattacks, and therefore require advanced approaches to risk management and system resilience. Accordingly, digital resilience extends the state of the art within resilience theory and, in this context, becomes an essential feature of any modern energy system. Given the foundational role of energy in supporting economic stability and long-term development, these components constitute priority areas for innovation and sustainability.

The studies by O. Trofymenko *et al.* (2021), H. Pudycheva (2021), and Yu. Kravchyk (2025) explored methodological approaches to the design of renewable energy infrastructure and assessed the prospects for further sustainable development in Ukraine and the European Union. Growing digitalisation simultaneously expands the cyber threat surface, creating systemic vulnerabilities that require coordinated resilience strategies. M.A. Alomari *et al.* (2025) emphasised the global importance of strengthening legislative and regulatory frameworks to enhance cybersecurity and operational resilience within the electricity sector. S. Horbachenko & O. Savratsky (2025) analysed strategies for proactively increasing resilience, including infrastructure redundancy, the implementation of cybersecurity frameworks, the diversification of energy resources, and the development of international cooperation aimed at strengthening the reliability and continuity of energy systems. Cybersecurity solutions provide mechanisms for detecting, preventing, and responding to cyber threats, thereby enhancing the resilience and operational stability of critical infrastructure.

A study by M. Florkowski *et al.* (2024) examined the functioning of the energy sector as a critical infrastructure for modern society, which relies heavily on the reliability of digital systems. The authors emphasise that the digitalisation of the energy sector, the introduction of automated solutions, and remote-control technologies are leading to increased complexity and vulnerability of energy systems. The study places particular emphasis on the role of AI technologies in improving the efficiency and resilience of energy systems, as well as new risks associated with cybersecurity, data integrity, and algorithmic decision-making. It is noted that disruptions in AI-driven energy systems can lead not only to economic losses but also to large-scale social risks.

S. Shandilya *et al.* (2024) examined the concept of system resilience in the context of digital transformation. Their research emphasises that different systems demonstrate varying capacities to withstand risks of diverse origins, adapt to environmental changes, and ensure rapid recovery while returning to a stable operational state. These capabilities are collectively conceptualised as resilience. The authors further argue that when such properties are achieved or enhanced through the adoption, implementation, and advancement of digital technologies, they can be defined as digital resilience, highlighting the critical role of digital tools and infrastructures in strengthening the adaptive and recovery capacities of modern systems.

Accelerating globalisation in the world economy, along with the liberalisation and integration of energy markets, increases the importance of research into mechanisms for ensuring energy security and supporting sustainable development in the energy sector. These processes create new challenges and interdependencies that require systematic analysis and coordinated action. In such conditions, the role of innovation management as a key tool for adapting energy systems to dynamic changes in the external environment is growing. Effective innovation management ensures the implementation of advanced technologies, in particular digital solutions, AI and cybersecurity systems, which contribute to increasing the resilience of energy infrastructure. Introduction of innovations is traditionally accompanied by uncertainty, but AI as a technological innovation has a qualitatively different risk profile.

Despite the growing body of research on cybersecurity, resilience, and digital transformation in the energy sector, several important aspects remain insufficiently explored. Existing studies primarily focus on the development of renewable energy infrastructure, regulatory frameworks, and cybersecurity strategies for protecting critical infrastructure. However, the specific mechanisms for integrating digital resilience principles into risk management processes in AI-related projects remain limited in the current literature. Therefore, the current research aimed to analyse the interplay between energy security and resilience of energy systems, explore the emerging risks associated with

digitalisation and implementation of intelligent systems, and evaluate managerial and policy measures necessary for the effective integration of AI in energy infrastructure.

Materials and Methods

The theoretical and methodological foundation of this study was grounded in the fundamental principles of economic theory and practice, as well as in a combination of general scientific and specialised methods for the analysis of economic phenomena. The methodological framework was based on an integrated approach that enables a comprehensive investigation of digital resilience and risk management in projects involving the application of AI within the energy sector. A set of general scientific methods, including scientific abstraction, analysis, and synthesis, was employed to conceptualise the research problem and to structure the theoretical framework. These methods facilitated the identification of key categories, relationships, and patterns associated with digital resilience, cybersecurity risks, and the integration of AI technologies into energy systems. In addition, historical and comparative analysis were applied to examine the evolution of approaches to resilience and energy security.

Comparative and logical analysis were specifically used to investigate the interrelationship between energy security and system resilience. The application of these methods enabled the alignment and critical evaluation of existing theoretical approaches and justified the need for their integration into modern risk management frameworks. A systems approach was adopted to consider digital resilience as an integral component of complex energy infrastructures. This approach allowed energy systems to be analysed as multi-level structures incorporating technological, organisational, and informational elements, thereby identifying the role of AI in enhancing system adaptability and recovery capacity. Economic and statistical methods were utilised to assess trends in the development of cyber threats and investments in cybersecurity. The empirical analysis was based on open-access statistical data, including materials from the State Service of Special Communications and Information Protection of Ukraine (n.d.), which were used to examine the dynamics of cyber incidents targeting the energy sector. Additionally, analytical reports from the Kyiv School of Economics (2024) and DTEK (2024) were employed to evaluate the economic losses and structural vulnerabilities of the Ukrainian energy system.

Trend analysis and graphical modelling were applied to visualise changes in the frequency of cyber incidents. Python-based data processing tools were used to construct time series and identify patterns and tendencies in the evolution of cyber threats. The use of these methods was justified by the need for quantitative validation of observed processes and for enhancing the analytical rigor of the study. Furthermore, the monographic method and thematic analysis were employed to examine a wide range of domestic and international scientific publications. A frequency-based content analysis of scholarly sources was conducted to identify dominant research themes, methodological approaches, and gaps in the existing literature on digital resilience, AI, and cybersecurity in energy systems. These sources formed the theoretical basis for the study and supported the development of the conceptual framework. Methods of induction, deduction, and synthesis were used to generalise the findings, formulate theoretical conclusions, and develop conceptual approaches to risk management in AI-related projects. The empirical basis of the study was represented by the energy sector of Ukraine, which is considered as a case study under conditions of heightened risk and wartime disruptions. This context provided a unique opportunity to analyse the functioning of critical infrastructure in crisis environments and to evaluate the role of digital technologies in ensuring system resilience. The research was conducted in several stages, including: analysis of theoretical approaches; collection and processing of statistical data; trend modelling and visualisation; and synthesis of results and development of a conceptual model of digital resilience.

Results and Discussion

AI-related innovation initiatives have traditionally been regarded as drivers of organisational complexity and potential vulnerability. This evolving understanding is encapsulated in the notion of digital resilience, which extends the classical concept of resilience – defined as a system's ability to absorb shocks, adapt to changing conditions, and recover from disruptions – by emphasising the enabling role of digital technologies and information systems within highly interconnected environments. Simultaneously, the ongoing digital transformation of critical infrastructures is fundamentally redefining governance and management paradigms, particularly in the energy sector. Digital resilience denotes the capability of energy systems to sustain stable and continuous operations under conditions of disruption, including cyber incidents, technological failures, and large-scale crisis events. The attainment of such resilience increasingly depends on the deployment of advanced analytical, monitoring, and automation technologies, with AI occupying a central role.

However, the integration of intelligent systems simultaneously generates new layers of operational, technological, and cybersecurity risk. These emerging risk profiles necessitate the implementation of structured and proactive risk management frameworks. Accordingly, effective governance of AI-related innovation projects requires the systematic alignment of AI capabilities with comprehensive risk assessment procedures, mitigation mechanisms, and resilience-oriented system architecture. Such an integrated approach is essential to ensuring the secure, reliable, and sustainable functioning of critical energy infrastructure in digitally transformed environments.

Innovation implementation is inherently associated with uncertainty and risk. AI represents a distinct class of innovation with risk characteristics. These risks include algorithmic opacity, data dependency, and ethical concerns.

Innovation implementation is inherently associated with uncertainty and risk, and AI represents a distinct class of innovation characterised by specific risk factors. Algorithmic opacity limits the interpretability of AI systems, data dependency makes their performance sensitive to the quality and completeness of datasets, and ethical concerns relate to fairness, privacy, and potential bias in automated decision-making. Together, these risks increase uncertainty in AI adoption and require careful governance to ensure responsible and reliable implementation. In innovation management, this necessitates the adaptation of classical risk management mechanisms. At the idea screening stage, additional evaluation criteria must be applied. These include data quality, model transparency, and potential societal impact. During the planning phase, technology readiness assessment becomes critical. This mechanism ensures alignment between AI solutions and organisational capabilities. In the development stage, agile methodologies enable iterative validation and risk reduction. Portfolio management mechanisms support risk diversification across AI projects. At the commercialisation stage, stakeholder management becomes essential due to regulatory and reputational risks. Continuous monitoring and post-implementation review ensure adaptive risk control.

The concept of energy security is closely linked to the notions of resilience and risk, both of which are fundamental to the stable and reliable operation of critical energy systems. The case of Ukraine between 2014 and 2021 illustrates a persistent imbalance between these dimensions. In 2014, the country exhibited moderate to high levels of risk alongside medium to low levels of resilience, a situation that showed little improvement over the subsequent six years. A significant external risk factor remained the country's dependence on energy imports, as four out of five major energy sources were imported. This dependency was further exacerbated by a high concentration of supplier power, stemming from limited diversification and the potential for politically motivated actions by exporting countries. At the same time, resilience factors were insufficient to offset these risks. Structural weaknesses – including underdeveloped infrastructure, outdated technologies, and inefficient, wasteful patterns of energy consumption – constrained the system's capacity to absorb and respond to external shocks (Chaika, 2023). Thus, in contemporary energy systems, resilience refers to the broader capacity of the system to anticipate, absorb, and recover from disruptions, including those arising from cyber threats. In this regard, resilience complements the concept of energy security by extending beyond the mere continuity of supply to encompass the system's ability to adapt and sustain functionality under adverse conditions.

The cybersecurity ecosystem in the energy sector encompasses a diverse set of stakeholders, including electric utilities, oil and gas corporations, renewable energy operators, transmission system operators, industrial automation vendors, cybersecurity solution providers, and national security agencies. Renewable energy operators, particularly those managing large-scale wind and solar installations, increasingly integrate cybersecurity measures to safeguard inverter technologies, distributed control systems, and remote monitoring platforms. This is crucial for maintaining the resilience of low-carbon energy systems and supporting the transition to sustainable energy models. The emergence of virtual power plants and peer-to-peer energy trading platforms further expands the cyber threat landscape, introducing new risks associated with decentralised and consumer-oriented infrastructures. Additionally, energy trading platforms and market participants are exposed to phishing, fraud, and insider threats, necessitating the implementation of advanced, finance-grade cybersecurity protocols. In the context of sustainable development, robust cybersecurity practices contribute to the stability, reliability, and trustworthiness of energy systems. Therefore, cybersecurity can be considered a foundational element of digital resilience, enabling the secure and sustainable evolution of modern energy ecosystems.

The cybersecurity ecosystem in the energy sector includes utilities, transmission system operators, technology vendors, cybersecurity providers, and government agencies, each performing roles in system operation, protection, regulation, and incident response while coordinating through shared platforms and protocols. The most common cyber threats include attacks on SCADA systems, malware, phishing, supply chain compromises, and vulnerabilities in distributed and decentralised energy infrastructures (Ige *et al.*, 2024). Practical cases have shown that cyberattacks can lead to power outages, disruption of fuel supply chains, and financial losses in energy markets. To mitigate these risks, organisations apply network segmentation, zero-trust approaches, continuous monitoring systems, and strict access control mechanisms. Altogether, these measures enhance digital resilience and ensure the stability and sustainability of modern energy systems.

Unprecedented missile strikes targeting key facilities of the electric power sector have resulted in widespread emergency power outages, the consequences of which have been mitigated through the extensive efforts of transmission system operators. Deliberate attacks on critical infrastructure, including power plants, substations, and transmission networks, have significantly undermined the stability and reliability of electricity supply. Despite these challenges, the energy sector has demonstrated a remarkable level of resilience, characterised by rapid resource mobilisation and the ability to restore system functionality under extreme conditions.

Emergency restoration mechanisms for electricity supply have been successfully implemented, enabling the gradual stabilisation of the power system. A historic milestone was achieved in 2022 with the synchronisation of the Ukrainian power system with the European electricity network. This integration strengthened energy security and created new opportunities for electricity trade. In addition, Ukraine expanded electricity exports to the European Union, thereby enhancing the country's position within the regional energy market (DTEK, 2024). Large-scale

disruptions to the power system required the deployment of structured resilience mechanisms combining technical recovery, coordinated system management, and adaptive infrastructure solutions. Restoration processes were organised in stages, including immediate fault isolation, activation of emergency protection schemes, and phased grid re-energisation, with priority given to critical facilities; in many cases, essential services were restored within one to three days. The transmission system operator Ukrenergo ensured continuous real-time coordination, balancing supply and demand, implementing controlled load shedding, and maintaining frequency stability under stressed conditions. Integration with ENTSO-E enabled cross-border electricity flows, with emergency imports reaching up to approximately 1-2 GW and covering a notable share of demand deficits during peak disruptions. Infrastructure resilience was further supported through the deployment of mobile substations, reserve generating capacities, and network reconfiguration, which contributed to the recovery of a substantial proportion of damaged assets and the stabilisation of overall system performance yberthreat-landscape-2024 (ENTSO-E strategic roadmap, n.d.).

The longitudinal analysis of cyber incidents targeting Ukraine's energy sector reveals a critical escalation in early 2024, where a sharp increase to 124 incidents (+138%) indicates the presence of a significant external destabilising factor or a shift in the monitoring paradigm that enhanced event detection. While the data reached a peak of 127 incidents in the second half of 2024, the subsequent stabilisation at 120 incidents in early 2025 suggests a transition toward a high-intensity plateau; consequently, a comparison of empirical data with the trend line indicates that, in the short-term perspective, incident frequency is projected to remain within the range of 115-125 cases per semi-annual period absent the implementation of further robust preventive measures (Fig. 1).

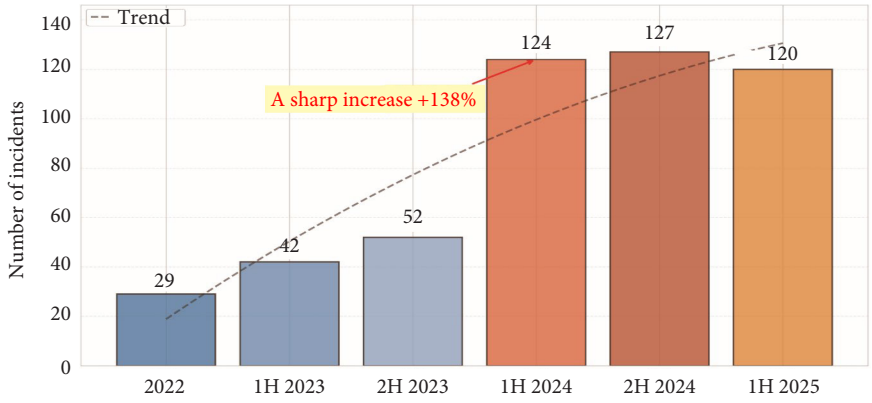

Figure 1. Trends in the number of cyber incidents targeting the energy infrastructure in Ukraine, 2022-2025
Source: prepared by the authors based on State Service of Special Communications and Information Protection of Ukraine (n.d.)

Between October 2022 and September 2024, the Russian Federation carried out more than 1000 attacks on Ukraine's energy infrastructure, damaging or destroying the majority of the country's major thermal and hydroelectric power plants. As a consequence of occupation and sustained military strikes during 2022-2023, the Ukrainian power system lost nearly 21 GW of generation capacity. In 2024 alone, the losses resulting from missile and drone attacks are estimated to exceed 9 GW (Kyiv School of Economics, 2024). In addition to generation facilities, repeated strikes have targeted critical nodes of the electricity transmission network, further increasing operational risks and placing additional pressure on the stability of the national energy system. One of the most significant applications of AI in energy resilience is predictive analytics for demand forecasting and operational planning. Machine learning models analyse historical consumption data, weather conditions, and economic indicators to forecast fluctuations in electricity demand. Such predictive capabilities allow system operators to optimise generation schedules and prevent overloads or shortages in energy supply. As a result, predictive analytics contributes to improved stability and efficiency in energy system operations. AI tools supporting digital resilience in energy systems are presented in Table 1.

Table 1. AI tools supporting digital resilience in energy systems

AI tool	Application in energy systems	Contribution to digital resilience
Predictive Analytics	Forecasting electricity demand and optimising generation planning	Improves system stability and prevents supply disruptions
Predictive Maintenance	Monitoring equipment condition using sensor data and AI models	Reduces equipment failures and unplanned outages
Anomaly Detection Systems	Identifying abnormal network behaviour and operational irregularities	Enhances cybersecurity and early threat detection
Decision Support Systems (AI-based)	Assisting operators in real-time operational and strategic decisions	Improves response speed and decision accuracy

Continued Table 1

AI tool	Application in energy systems	Contribution to digital resilience
Digital Twins	Creating virtual models of energy infrastructure for simulation	Enables risk modelling and scenario testing
Smart Grid Optimisation Algorithms	Managing distributed energy resources and balancing loads	Enhances grid flexibility and operational efficiency
Renewable Energy Forecasting Models	Predicting solar and wind generation levels	Supports integration of renewable energy sources
Automated Control Systems	Real-time adjustment of energy flows and grid parameters	Ensures rapid adaptation to system disturbances

Source: prepared by the authors based on F. Bertone *et al.* (2020), J. Holmström (2022), A. Sulaiman *et al.* (2023), J. Ruan *et al.* (2023), P. Koundouri *et al.* (2025), S.C. Vetrivel *et al.* (2025), H. Dui *et al.* (2025), M.F. Khaleel & Z.M. Abdulkareem (2025)

Another critical area of AI application is predictive maintenance of energy infrastructure. Intelligent algorithms process large volumes of sensor data collected from turbines, transformers, and transmission lines to detect early signs of equipment degradation or malfunction. By identifying potential failures before they occur, AI systems allow energy companies to implement preventive maintenance strategies and reduce the risk of unexpected outages. This approach enhances operational reliability while simultaneously lowering maintenance costs and extending the lifespan of critical assets.

AI also plays an essential role in strengthening the cybersecurity and operational monitoring of digitalised energy systems. Advanced anomaly detection algorithms continuously analyse network activity and system performance to identify irregular patterns that may indicate cyber intrusions or technical faults. Through real-time monitoring and automated alerts, these systems enable rapid response to potential threats and help prevent cascading failures within interconnected energy networks. Furthermore, AI-driven decision support systems and digital twin technologies provide advanced tools for modelling, simulation, and strategic planning in the energy sector. Digital twins create virtual representations of physical energy infrastructure, allowing operators to simulate various operational scenarios and evaluate potential risks. Combined with AI-based decision support systems, these tools improve situational awareness and facilitate data-driven decision-making. Consequently, the integration of AI technologies significantly contributes to the development of resilient, adaptive, and secure energy systems.

Cyber risks in the energy sector range from malware and ransomware to sophisticated state-sponsored attacks targeting operational technology and industrial control systems. The consequences of such attacks may include power outages, equipment damage, financial losses, and reduced public trust in energy providers. The integration of renewable energy sources and smart grid technologies further increases the complexity of the system, creating new potential attack vectors. Effective mitigation requires a combination of robust cybersecurity strategies, continuous monitoring, staff training, and the adoption of advanced technologies such as AI for threat detection and predictive maintenance.

The global cybersecurity market in the energy sector generated approximately USD 8.6 billion in revenue in 2021. This market is expected to experience substantial growth over the coming decade as the digitalisation of energy infrastructure accelerates and cyber threats continue to intensify. According to current projections, the market volume is anticipated to reach nearly USD 21.8 billion by 2031. This growth corresponds to an average annual growth rate of approximately 11.3% during the period from 2022 to 2031 (Allied Market Research, n.d.). The expansion of cybersecurity investments reflects the increasing priority placed on protecting critical energy infrastructure and ensuring the stability and resilience of modern power systems.

It is emphasised that it is necessary to help managers and other decision-makers make informed investment decisions to effectively ensure IT security. The study addresses issues such as lack of transparency in IT security costs, staff shortages and difficulties in resource planning. A sample calculation shows the financial impact of IT security measures using the Return on Security Investment (RoSI) model (Deutsche Energie-Agentur, n.d.). The RoSI cost estimate shows that the investment is already profitable for important companies in the first year, and for particularly important ones – from the second year. The sample calculation illustrates that the investment is profitable even with low damage compensation costs.

The development of national strategies for the digital transformation of the energy sector, alongside the implementation of industry standards and regulatory frameworks for the safe and ethical use of AI, facilitates the formalisation of digital processes. Such regulatory support also encompasses the establishment of quality control mechanisms, certification of innovative products, licensing of AI-based solutions, and assurance of consumer data protection. Financial and investment incentives are critical for fostering the adoption of innovative solutions by energy companies. These mechanisms include government subsidies, grants, concessional loans, and tax incentives aimed at encouraging investment in digital modernisation. An essential component of this approach is the promotion of public-private partnerships, which enable the pooling of resources from governmental bodies, private enterprises, and research institutions to implement large-scale technological initiatives.

The investment feasibility of cybersecurity solutions based on AI is determined by their capacity to enhance digital resilience. AI-driven systems enable proactive

threat detection and real-time response. This reduces the expected losses from cyber incidents. In the framework of innovation management, such investments should be evaluated using risk-adjusted performance metrics. Traditional cost-benefit analysis is insufficient for AI-based cybersecurity solutions. It should be complemented by scenario analysis and probabilistic risk assessment. The incorporation of AI improves the accuracy of threat intelligence and forecasting models. This increases the effectiveness of resource allocation in cybersecurity strategies. However, investment decisions must account for implementation risks, including model bias and data vulnerabilities. Regulatory compliance and ethical considerations also influence the overall investment attractiveness. Therefore, a comprehensive evaluation approach is required to ensure sustainable and resilient AI-driven cybersecurity investments.

In the energy sector, several factors act as barriers to technological change. A conservative approach to adopting new technologies is often driven by concerns regarding their effectiveness and potential impact on existing business models. Additionally, digital transformation initiatives in many energy companies remain incomplete, necessitating further investment and the restructuring of management practices. Management is evolving from a primarily administrative and control-oriented function into an intelligent, analytical mechanism for strategic coordination, which integrates human expertise with algorithmic analytics. The ultimate objective is to establish an effective, adaptive, and transparent decision-making framework that combines human experience with the capabilities of analytical algorithms through a comprehensive controlling system.

The human factor continues to represent one of the primary challenges for energy enterprises, as the resilience of operational technology systems and energy networks depends largely on employee actions in mitigating both external and internal cyber threats. Currently, there is a pronounced shortage of cybersecurity specialists, which poses a significant challenge for the sector. The Figure 2 illustrates the key challenges associated with the implementation of AI, including regulatory gaps, transparency issues, hybrid threats, and human-factor risks. It also presents sustainability strategies such as AI-blockchain synergy, structured threat taxonomies, and safety culture, which support the development of digital resilience and effective risk management in AI-related projects.

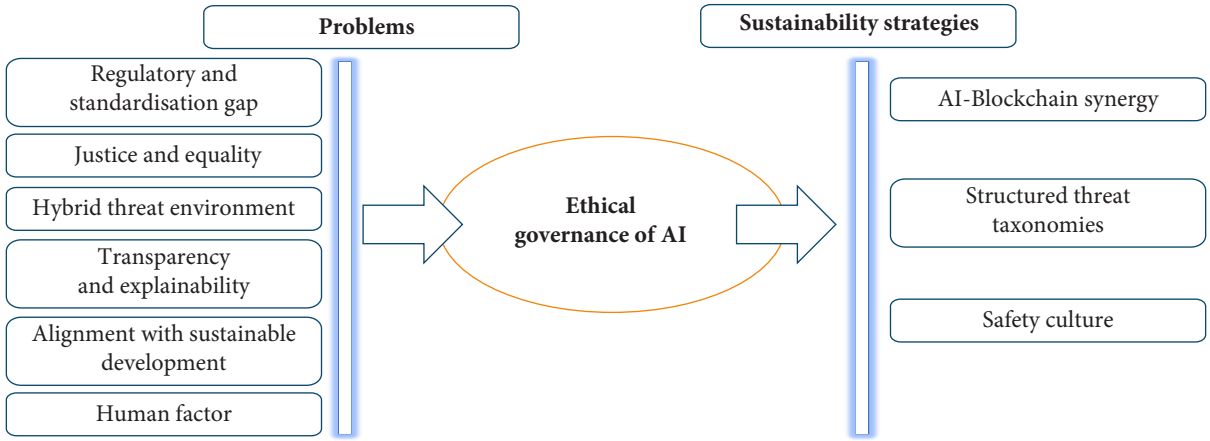

Figure 2. Conceptual framework of ethical AI governance for digital resilience and risk management in AI-related projects

Source: prepared by the authors

Scientific, educational, and workforce development further ensure the creation of a professional foundation for the effective utilisation of AI tools within the energy sector. Supporting specialised educational programs in digital technologies, particularly those focused on energy systems, is essential for preparing qualified personnel. Moreover, initiatives should promote the retraining of existing energy sector employees and the establishment of research centres and laboratories dedicated to the development and implementation of AI solutions for energy infrastructure. The deployment of comprehensive cybersecurity solutions across energy infrastructure requires substantial financial investment, reflecting the critical importance of safeguarding complex and digitally integrated energy systems. Building on the challenges and strategies highlighted in the figure, Table 2 provides a detailed overview of the economic effects of AI applications in the energy sector. It summarises key application areas, the mechanisms through which AI generates value, and the expected outcomes for operational efficiency, cost reduction, and strategic decision-making. The Table 2 summarises key AI application areas, the associated economic effects, the mechanisms through which AI generates value, and the expected outcomes for energy systems, including cost reduction, improved efficiency, risk mitigation, and enhanced decision-making. Ukraine demonstrates considerable development potential due to its unique experience in countering cyber warfare, the rapid pace of digital trans-

formation, and the strong support of international partners. At the same time, the sector remains vulnerable due to market fragmentation, insufficient systemic financing, and the lack of comprehensive regulatory and legal standards for businesses operating in the digital environment. Nevertheless, the growing demand for cybersecurity solutions, the diversification of technological capabilities, and the potential for exporting digital technologies create favourable conditions for Ukraine to evolve into a regional leader in this domain.

Table 2. Economic effects of AI applications in the energy sector, their value creation mechanisms, and expected outcomes

AI application area	Economic effect	Mechanism of value creation	Expected outcome
Predictive Maintenance	Reduction of maintenance costs	Early detection of equipment failures through data analytics	Decreased downtime, extended asset lifetime
Demand Forecasting	Optimisation of energy production costs	Accurate prediction of consumption patterns using machine learning models	Reduced imbalance costs and improved planning efficiency
Smart Grid Management	Improved operational efficiency	Real-time load balancing and automation of grid operations	Lower transmission losses and increased system stability
Cybersecurity (AI-based)	Risk cost reduction	Early detection of cyber threats and automated response	Prevention of financial losses from cyber incidents
Renewable Energy Optimisation	Increased return on investment (ROI)	Forecasting of renewable generation and integration into energy systems	Higher utilisation of renewable sources and reduced curtailment
Energy Management Systems	Cost savings in energy consumption	AI-driven optimisation of industrial and commercial energy use	Reduced energy expenses and improved efficiency
Decision Support Systems	Improved investment decision quality	Data-driven analysis of scenarios and risks	More efficient capital allocation and reduced uncertainty
Digital Twins	Cost reduction in system testing and planning	Simulation of operational scenarios and risk modelling	Lower costs of errors and improved infrastructure planning

Source: prepared by the authors

Overcoming these structural barriers requires the coordinated integration of education, business, and public policy into a unified system aimed at strengthening national cyber resilience. However, alongside these opportunities, new challenges are emerging. The widespread adoption of digital technologies and AI raises critical questions regarding ethical governance, the development of transparent and accountable algorithmic decision-making systems, and the fair allocation of responsibility among technology developers, system operators, and regulatory authorities. These challenges are particularly acute in sectors that have experienced the most significant physical and cyber impacts in recent years, most notably the Ukrainian energy sector. Ensuring the resilience of this sector requires the implementation of innovative protection strategies, continuous professional development of specialised personnel, and the cultivation of a culture of digital responsibility among all stakeholders involved in the energy ecosystem.

Overall, the analysis of the reviewed studies demonstrated a strong and growing consensus regarding the critical role of artificial intelligence and cybersecurity in enhancing the resilience of modern energy systems. The existing literature confirmed that increasing digitalisation, while enabling significant efficiency gains, simultaneously introduced new layers of complexity and vulnerability. The technological dimension of resilience was explored in detail in several studies. Specifically, M. Shadabfar *et al.* (2022) highlighted the importance of resilience-oriented design frameworks incorporating computational models and simulation tools to anticipate and withstand disruptions. The findings of the study aligned with this conclusion regarding the need for proactive modelling; however, this perspective was expanded in the current study by demonstrating that such technological frameworks must be an integral part of a comprehensive risk management system. Similarly, I. Alhamrouni *et al.* (2024) emphasised the role of artificial intelligence in enhancing system stability through real-time control, fault detection, and adaptive protection mechanisms. Conclusions fully corroborated the effectiveness of AI tools for monitoring and predictive analytics, but additionally indicated that technical robustness must be supported by organisational adaptability. Furthermore, B. Ozpineci (2022) examined the integration of AI and machine learning techniques directly into power electronics and cybersecurity architectures. Current results coincided with the author's vision regarding the formation of the technological core of resilient energy systems; nevertheless, the necessity of combining these architectures with institutional governance mechanisms was emphasised.

However, a purely technological approach appeared insufficient to fully capture the complexity of the contemporary energy environment. The research by S.M. Stezhko & V.M. Fitsa (2021) highlighted the institutional and regulatory dimensions, arguing that the effectiveness of cybersecurity measures depended on national policies and legal frameworks. The conclusions of current study agreed with this assertion, as regulatory compliance and stakeholder coordination were also considered as mandatory

components of the proposed integrated model of digital resilience. Along the same lines, A. Ige *et al.* (2024) demonstrated that the implementation of cyber risk defence strategies required the alignment of technical solutions with organisational processes and human resource capabilities. This conclusion completely coincided with the results obtained, which confirmed the necessity of a systemic approach wherein technological innovations were supported by managerial mechanisms.

Recent empirical data also pointed to a critical gap between theoretical advancements and practical implementation. M. Nachaat *et al.* (2023) noted that energy enterprises faced barriers such as high implementation costs, a lack of technical expertise, and organisational inertia. Results fully aligned with these observations, confirming that the transition from the technological potential of AI to its practical application was significantly constrained by structural and managerial factors. Similarly, O. Degtiareva *et al.* (2024) highlighted the limited integration of AI-based cybersecurity tools into operational processes, particularly in regions with economic constraints. The findings of the study coincided with this position; however, a specific mechanism to overcome this issue through the implementation of a comprehensive risk management framework was also proposed.

Despite the alignment of results with the conclusions of the aforementioned scholars in specific aspects, the comparative analysis revealed a fundamental limitation in the existing literature. Most prior studies tended to examine technological, infrastructural, or policy-related aspects in isolation, without adequately addressing their interdependencies. In contrast to this fragmented approach, the results of current research substantiated the need for an integrated analytical framework. The model extended existing approaches by explicitly linking AI capabilities with structured risk management processes (including risk identification, assessment, mitigation, and continuous monitoring) within a unified conceptual model of digital resilience. Thus, the results of this work confirmed that the future development of energy systems required a paradigm shift from isolated technological solutions toward comprehensive, risk-oriented management models that balanced innovation, institutional governance, and human capital development in the face of hybrid threats.

Conclusions

The study demonstrates that the sustainable development of modern energy systems is fundamentally dependent on minimising operational and systemic risks associated with cyber threats. Any destabilisation of critical energy infrastructure significantly reduces both the environmental and economic efficiency of the sector, thereby confirming that cybersecurity has become an integral component of sustainable energy governance. The research results indicate that the implementation of intelligent technologies, particularly AI-based systems, plays a key role in strengthening innovation-driven management in the energy sector. At the same time, the increasing digitalisation of energy infrastructure leads to higher exposure of information and communication systems to a wide range of cyberattacks. Once deployed, such systems remain continuously vulnerable to external interference, which makes resilience and survivability essential characteristics of modern energy information systems. It has been established that ensuring the stable functioning of energy infrastructure under adverse and uncertain conditions requires a systemic approach to digital resilience management. This approach integrates technological, organisational, and strategic components into a unified governance framework. Effective cybersecurity governance must clearly define responsibilities across all management levels, ensuring coordination in cybersecurity operations, business continuity planning, and incident response mechanisms.

The study highlights the importance of combining continuous monitoring, real-time threat detection, and predictive analytics with structured risk assessments and scenario-based testing. Such integration enhances the adaptive capacity and robustness of energy systems. Additionally, human-centred measures, including training, awareness programs, and adaptive operational procedures, significantly reduce vulnerabilities caused by human factors. Empirical evidence from Ukraine confirms that the combined application of technological solutions, organisational coordination, and strategic management enables energy systems to maintain functionality even under extreme conditions. In this context, AI-based tools for anomaly detection and predictive control further strengthen proactive risk management within energy enterprises. Future development of energy systems should be based on an integrated resilience-oriented approach, where digital security is embedded into overall sustainability strategies. The formation of a resilience ecosystem, supported by standardised indicators, AI-driven mitigation mechanisms, and international cooperation frameworks, is essential for ensuring the stability and security of interconnected global energy networks.

Acknowledgements

None.

Funding

This research was supported by the Artificial Intelligence Centre and the specialised laboratory "Cyber Polygon" of the National University "Odesa Law Academy" (Ukraine). Additional support was provided within the framework of the research project "Digitalisation Scenario of the 5D Energy Transition in the Ukrainian Energy Sector", funded by the Alexander von Humboldt Foundation (Germany).

Conflict of Interest

None.

References

[1] Alhamrouni, I., Abdul Kahar, N.H., Salem, M., Swadi, M., Zahraoui, Y., Kadhim, D.J., Mohamed, F.A., & Alhuyi Nazari, M. (2024). A comprehensive review on the role of artificial intelligence in power system stability, control, and protection: Insights and future directions. *Applied Sciences*, 14(14), article number 6214. doi: 10.3390/app14146214.

[2] Allied Market Research. (n.d.). *Cyber-security in energy market to reach $21.8 billion globally by 2031 at 11.3% CAGR*. Retrieved from https://surl.li/xmeetn.

[3] Alomari, M.A., Al-Andoli, M.N., Ghaleb, M., Thabit, R., Alkawsi, G., Alsayaydeh, J.A.J., & Gaid, A.S.A. (2025). Security of smart grid: Cybersecurity Issues, potential cyberattacks, major incidents, and future directions. *Energies*, 18(1), article number 141. doi: 10.3390/en18010141.

[4] Bertone, F., Lubrano, F., & Goga, K. (2020). Artificial intelligence techniques to prevent cyber attacks on smart grids. *Annals of Disaster Risk Sciences*, 3(1). doi: 10.51381/adrs.v3i1.42.

[5] Chaika, O. (2023). *Russian hackers coordinate actions with the military and intensify attacks on the eve of winter. How Ukraine resists cyberattacks on the power system*. Retrieved from https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242.

[6] Deutsche Energie-Agentur. (n.d.). *Cyber-Fit: Investing in cybersecurity in the electricity industry*. Berlin: Deutsche Energie-Agentur GmbH (dena).

[7] DTEK. (2024). *Action report 2024: Fight for light*. Retrieved from https://www.dtek.com/en/media-centre/publications.

[8] Dui, H., Zeng, Q., & Xie, M. (2025). Generative AI-based spatiotemporal resilience, green and low-carbon transformation strategy of smart renewable energy systems. *Frontiers of Engineering Management*, 12, 1220-1235. doi: 10.1007/s42524-025-4147-6.

[9] ENTSO-E strategic roadmap. (n.d.) Retrieved from https://www.entsoe.eu/.

[10] Florkowski, M., Hayashi, H., Matsuda, S., Moribe, H., Moriwaki, N., Jones, D., & Pauska, J. (2024). Digitally boosted resilience: Digitalization to enhance resilience of electric power system. *IEEE Power and Energy Magazine*, 22(2), 100-109. doi: 10.1109/MPE.2023.3344554.

[11] Horbachenko, S., & Savratskiy, O. (2025). Transformation of the innovative component of management processes in the context of digitalization. *Pryazovskyi Economic Herald*, 3(43), 62-68. doi: 10.32782/2522-4263/2025-3-11.

[12] Ige, A.B., Kupa, E., & Ilori, O. (2024). Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources. *International Journal of Science and Research Archive*, 12(1), 2978-2995. doi: 10.30574/ijsra.2024.12.1.1186.

[13] Khaleel, M.F., & Abdulkareem, Z.M. (2025). A study on the role of artificial intelligence and renewable energy technologies in building a sustainable future. *Journal of Artificial Intelligence, Machine Learning and Neural Network*, 51(1), 14-27. doi: 10.55529/jaimlnn.51.14.27.

[14] Koundouri, P., Feretzakis, G., & Alamanos, A. (2025). *Integrating AI into energy systems: The approach of the Global Climate Hub*. Retrieved from https://wpa.deos.aueb.gr/docs/2025.Global.Climate.Hub.AI.pdf.

[15] Kravchyk, Yu. (2025). Strategic planning of hydrogen economy development in the context of Ukraine's energy transition. *Ukrainian Journal of Applied Economics and Technology*, 10(1), 40-45. doi: 10.36887/2415-8453-2025-1-6.

[16] Kyiv School of Economics. (2024). *Damages and losses of the energy sector of Ukraine*. Kyiv: Kyiv School of Economics.

[17] Nachaat, M., Oubelaid, A., & Almazrouei, S. (2023). Staying ahead of threats: A review of AI and cyber security in power generation and distribution. *International Journal of Electrical and Electronics Research*, 11(1), 143-147. doi: 10.37391/IJEER.110120.

[18] Ozpineci, B. (2022). AI/ML and cybersecurity in power electronics. *IEEE Power Electronics Magazine*, 9(4), 38-40. doi: 10.1109/MPEL.2022.3222584.

[19] Pudycheva, H. (2021). The structure of energy supply chains in Ukraine. *Tavria Scientific Bulletin. Series: Economics*, 5, 72-82. doi: 10.32851/2708-0366/2021.5.9.

[20] Ruan, J., Liang, G., Zhao, J., Zhao, H., Qiu, J., Wen, F., & Dong, Z.Y. (2023). Deep learning for cybersecurity in smart grids: Review and perspectives. *Energy Conversion and Economics*, 4(4), 233-251. doi: 10.1049/enc2.12091.

[21] Shadabfar, M., Mahsuli, M., Zhang, Y., Xue, Y., Ayyub, B.M., Huang, H., & Medina, R.A. (2022). Resilience-based design of infrastructure: Review of models, methodologies, and computational tools. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, 8(1), article number 03121004. doi: 10.1061/AJRUA6.0001184.

[22] Shandilya, S.K., Datta, A., Kartik, Y., & Nagar, A. (2024). What is digital resilience? In *Digital resilience: Navigating disruption and safeguarding data privacy* (pp. 3-42). Cham: Springer. doi: 10.1007/978-3-031-53290-0_1.

[23] State Service of Special Communications and Information Protection of Ukraine. (n.d.). Retrieved from https://cip.gov.ua/ua.

[24] Stezhko, S.M., & Fitsa, V.M. (2021). Cybersecurity as an important factor in ensuring the vital activity of the domestic energy industry. *Information and Law*, 4(39), 113-120. doi: 10.37750/2616-6798.2021.4(39).248828.
[25] Sulaiman, A., Nagu, B., Kaur, G., Karuppaiah, P., Alshahrani, H., Reshan, M.S., & Shaikh, A. (2023). Artificial intelligence-based secured power grid protocol for smart city. *Sensors*, 23(19), article number 8016. doi: 10.3390/s23198016.
[26] Trofymenko, O., Shevchuk, O., Koba, N., Tashcheiev, Y., & Pavlenco, T. (2021). Knowledge and innovation management for transforming the field of renewable energy. In *Artificial intelligence and sustainable computing for smart city* (pp. 73-87). Cham: Springer. doi: 10.1007/978-3-030-82322-1_6.
[27] Vetrivel, S.C., Arun, V.P., Saravanan, T.P., Maheswari, R., & Mohanasundari, M. (2025). Socio-economic impacts of digital innovations in renewable energy adoption. In J.K.P. Mukthar, V. Jain, S.B. Tsai & C.H. Wu (Eds.), *Digital innovations for renewable energy and conservation* (pp. 277-312). Hershey: IGI Global Publishing. doi: 10.4018/979-8-3693-6532-8.ch012.

Ризик-орієнтоване управління продуктовими AI-рішеннями в енергетичній галузі

Ольга Дегтярьова
Доктор економічних наук, професор
Університет прикладних наук Мітвайда
09648, Технікумплац, 1, м. Міттвайда, Німеччина
Одеський національний економічний університет
65082, вул. Преображенська 8, м. Одеса, Україна
https://orcid.org/0000-0003-1276-334X

Тетяна Куклінова
Кандидат економічних наук, доцент
Національний університет «Одеська юридична академія»
65009, вул. Фонтанська дорога, 23, м. Одеса, Україна
https://orcid.org/0000-0002-1370-2883

Валерія Слатвінська
Доктор філософії у галузі права, викладач
Національний університет «Одеська юридична академія»
65009, вул. Фонтанська дорога, 23, м. Одеса, Україна
https://orcid.org/0000-0002-6082-981X

Володимир Гура
Кандидат технічних наук, доцент
Національний університет «Одеська юридична академія»
65009, вул. Фонтанська дорога, 23, м. Одеса, Україна
https://orcid.org/0000-0001-6415-7865

Олександр Задерейко
Кандидат технічних наук, доцент
Національний університет «Одеська юридична академія»
65009, вул. Фонтанська дорога, 23, м. Одеса, Україна
https://orcid.org/0000-0003-0497-9861

Анотація. Інноваційні ініціативи, пов'язані зі штучним інтелектом, в енергетичному секторі традиційно розглядалися як джерела організаційної складності та потенційної вразливості. Метою дослідження було проаналізувати взаємодію між енергетичною безпекою та стійкістю енергетичних систем, дослідити нові ризики, пов'язані з цифровізацією та впровадженням інтелектуальних систем, а також оцінити управлінські та політичні заходи, необхідні для ефективної інтеграції штучного інтелекту в енергетичну інфраструктуру. Для досягнення поставлених цілей використано джерела з відкритим доступом та застосовано інтегрований підхід, що поєднує загальнонаукові й спеціалізовані методи дослідження з акцентом на передові аналітичні, моніторингові та автоматизовані технології. Результати дослідження підкреслюють важливість інвестування в технологічний, людський та регуляторний потенціал для повного використання потенціалу штучного інтелекту. Водночас роль інструментів на базі штучного інтелекту в сучасних енергетичних системах зростає завдяки їхньому внеску в

цифрову стійкість, операційну стабільність, прогнозне обслуговування, кібербезпеку та прийняття стратегічних рішень. Однак ці розробки супроводжуються відповідними ризиками. Саме тому сучасна система управління повинна еволюціонувати від адміністративної та контрольно-орієнтованої функції до інтелектуального аналітичного механізму, який інтегрує людський досвід з алгоритмічним прийняттям рішень. Таким чином, цифрова стійкість розширює концепцію стійкості системи, інтегруючи інформаційні технології та аналітику на основі штучного інтелекту для передбачення, поглинання та відновлення після збоїв, спричинених фізичними, технологічними чи кіберінцидентами. Ця інтеграція зменшує суб'єктивність, підвищує точність операційних рішень та забезпечує прозорий, адаптивний та науково обґрунтований підхід до стратегічної координації. Поєднуючи передову аналітику, автоматизацію на основі штучного інтелекту та проактивне управління ризиками, енергетичні системи можуть досягти підвищеної стабільності, експлуатаційної надійності та стійкості до кібербезпеки у все більш складних та цифрово взаємопов'язаних середовищах. Крім того, використання передового світового досвіду та сприяння транскордонній співпраці в галузі інновацій у сфері штучного інтелекту та кібербезпеки може прискорити трансформацію енергетичних підприємств у напрямку стійких, інтелектуальних та стійких інфраструктур

Ключові слова: цифрове середовище; кіберризики; інвестиції; продакт менеджмент; стратегічне планування; управління проектами; операційний ризик