УДК 005.334:656.025.4
UDC 005.334:656.025.4

Tsopa V.[1], Cheberyachko S.[2], Deryugin O.[2], Litvinova Ya.[2], Klymenko I.[2]
Private Higher Educational Institution «International Management Institute (MIM-Kyiv)»[1]
Dnipro University of Technology[2]

IMPROVEMENT OF THE LOGISTICS RISK MANAGEMENT PROCESS FOR CRITICAL INFRASTRUCTURE ENTERPRISES

Supply chains of critical infrastructure enterprises under contemporary conditions are characterized by high complexity, digitalization, and an increasing level of hybrid threats, which necessitates a transition from reactive to proactive approaches to logistics risk management. The purpose of this article is to improve the logistics risk management process within supply chain security management systems of critical infrastructure facilities through the implementation of the requirements of the international standard ISO 28000:2022.

The study employs systems analysis to examine supply chains as complex, interconnected ecosystems, as well as methods of mathematical and logical modeling to formalize risk assessment as a function of the probability of threat realization and the severity of its consequences. An improved logistics risk management process is proposed, based on the integration of the requirements of ISO 28000:2022, ISO 31000:2018, and ISO/IEC 27001:2022, with mandatory consideration of risks associated with the use of artificial intelligence in accordance with ISO/IEC 42001.

The improved process includes context definition and supply chain mapping using artificial intelligence tools; identification of assets and sources of threats with consideration of AI models and datasets; vulnerability analysis and assessment of incident probability; consequence analysis taking into account ethical and social AI risks; scenario simulation; development of security plans and risk treatment; as well as continuous system improvement considering the evolution of digital technologies. Practical implementation of the proposed approach is aimed at enhancing the resilience of critical infrastructure supply chains under conditions of dynamic risks and accelerated digitalization.

Keywords: ISO 28000, critical infrastructure, logistics risk management, supply chain resilience, integrated management systems, cyber-physical convergence, infrastructure decentralization, business continuity.

INTRODUCTION

In the contemporary, highly interconnected and globalized macroeconomic system, supply chains function as the fundamental circulatory system of any modern state. They ensure the continuity of production processes, the provision of basic social services, and the stable functioning of society as a whole. Critical infrastructure enterprises including the energy, transport, healthcare, and food sectors, as well as telecommunications and water supply, are in a state of tense, almost existential dependence on the reliability and uninterrupted operation of their logistics networks [1]. The growing complexity of these networks, currently characterized by deep technological and geographical interdependence, along with exposure to multifaceted and often unpredictable risks, necessitates an urgent shift from fragmented, reactive security measures to a highly integrated, proactive, and holistic approach to corporate governance [2].

Disruptions in global and local supply chains caused by geopolitical conflicts, large-scale cyberattacks, destructive natural disasters, industrial accidents, or pandemics are capable of triggering so-called cascading effects [1]. The phenomenon of cascading effects lies in the fact that disruption of even the smallest node in a logistics network inevitably leads to a domino effect, resulting in the shutdown of critical services at national or even transnational levels [3]. In this context, modern logistics management goes far beyond the traditional paradigm of physical asset protection and transforms into a complex strategic initiative aimed at ensuring continuous operational resilience of enterprises [4]. Achieving such resilience requires the development of multilevel strategies that take into account the interests of all stakeholders, from raw material suppliers to end users of critical services.

Accordingly, a pressing scientific and practical problem is the development and implementation of effective logistics risk management within supply chain security management systems of critical infrastructure facilities through the systematic implementation of the requirements of the international standard ISO 28000:2022 “Security and resilience – Security management systems for the supply chain – Requirements with guidance for use.” Implementation of this standard makes it possible to transition from reactive to proactive risk management, ensure the integration of security processes across all links of the logistics chain, and achieve compliance with resilience and security requirements of critical infrastructure facilities under contemporary challenges.

LITERATURE REVIEW AND PROBLEM STATEMENT

To build a supply chain resilience architecture, a family of international ISO 28000 standards has been developed, providing a comprehensive and scientifically grounded framework for identifying vulnerabilities

and for establishing, implementing, operating, reviewing, maintaining, and continuously improving supply chain security management systems [6]. Implementation of this system enables organizations not only to protect their assets from malicious actions, but also to develop flexible mechanisms for adapting to crisis conditions while maintaining operational profitability and preserving trust from society and the state [7].

Supply chain management has undergone unprecedented digitalization. Modern logistics processes of critical infrastructure are governed by complex software systems, cloud computing, and artificial intelligence (AI) algorithms used for dynamic routing of transport flows, intelligent demand forecasting, and automated customs clearance [8]. This technological evolution has created an entirely new class of logistics risks driven by the phenomenon of cyber-physical convergence, whereby virtual attacks on information systems are instantly materialized in the form of physical disruptions on transport corridors or in energy networks [9].

For critical infrastructure enterprises, logistics risk management is further complicated by the introduction of new, stringent European regulatory frameworks, including the NIS2 Directive (on a common high level of cybersecurity), the CER Directive (on the resilience of critical entities), and the European Cyber Resilience Act (CRA) [10]. As traditional physical security standards often prove to be “blind” to algorithmic threats, contemporary research proposes comprehensive multi-stage models for managing supply chain security and AI-related risks. Applying the logic of ISO 28000, strict supplier tiering is introduced, based not on the financial volume of contracts but exclusively on the criticality of contractors and their ability to trigger cascading impacts on essential services (for example, a regional blackout caused by a failure in the software of a transformer supplier) [2].

PURPOSE AND OBJECTIVES OF THE STUDY

The purpose of the study is to improve the logistics risk management process within supply chain security management systems of critical infrastructure facilities through the implementation of the requirements of ISO 28000:2022.

The study employs a combination of general scientific and specialized methods, including systems analysis to examine supply chains of critical infrastructure as complex, interconnected ecosystems, as well as mathematical and logical modeling to formalize risk assessment as a function of the probability of threat realization and the severity of its consequences.

RESEARCH RESULTS

Effective and comprehensive logistics risk management requires a deep understanding of the entire ecosystem of related standards. Although ISO 28000 is the core regulatory document that establishes direct certification requirements, it is organically supported by a set of auxiliary guidelines (Table 1), each of which performs a specific function in building a resilient enterprise.

Table 1. ISO 28000 Family of Standards: Requirements and Guidelines

Standard	Title and Scope	Current Status and Functional Role in the Management Architecture
ISO 28000:2022	Security and resilience – Security management systems for the supply chain – Requirements	Active. This is the core standard establishing fundamental requirements for the Supply Chain Security Management System (SCSMS) applicable to the entire organization, including all links of its supply chain [7].
ISO 28001:2007	Supply chain security management systems – Best practices for implementation, assessments, and plans	Active. Provides a detailed step-by-step methodology for risk assessment, development of comprehensive security plans, and achievement of compliance with the strict criteria of the Authorized Economic Operator (AEO) [11].
ISO 28002:2011	Development of resilience in the supply chain – Requirements with guidance for use	Withdrawn (repealed in 2024). Despite its formal withdrawal, its fundamental principles have been organically integrated into ISO 28000:2022, and the concepts of organizational resilience remain fully relevant for practical application during audits and tenders [12].
ISO 28003:2007	Requirements for bodies providing audit and certification of supply chain security management systems	Active. This standard ensures standardized approaches to external auditing, thereby enhancing global trust in ISO 28000 certification through regulation of auditor competence [10].
ISO	Guidelines on the	Active. The standard consists of several parts, including general

28004:2007	implementation of ISO 28000	principles (Part 1) and specific guidance for adapting requirements for small and medium-sized seaports (Part 2), other enterprises (Part 3), and integration with ISO 28001 (Part 4) [12].

The full strategic potential of implementing ISO 28000:2022 can be realized only when it is deeply harmonized with other corporate management systems. Modern global supply chains, characterized by high dynamism, require the establishment of Integrated Management Systems (IMS). The implementation of the IMS approach enables organizations to avoid duplication of bureaucratic processes, optimize resource utilization, and break down operational "silos" in which different departments (security, quality, environmental management) operate in isolation from one another [3].

The specific nature of critical infrastructure operations requires simultaneous consideration of multiple risk vectors. For example, integrating the requirements of ISO 28000 with those of ISO 9001 (quality management systems) ensures not only continuity of product deliveries but also guarantees the preservation of product quality characteristics during transportation, which is particularly critical for pharmaceutical logistics and food transport [3]. The combined application of ISO 14001 (environmental management) and ISO 45001 (occupational health and safety management) is essential to ensure the safe transportation and storage of hazardous goods (e.g., water treatment chemicals or fuels for the energy sector), while simultaneously protecting personnel and the environment from potential leaks or acts of sabotage [13].

Of particular strategic importance for critical infrastructure enterprises is the deep synchronization of ISO 28000 processes with the requirements of ISO 31000 (risk management) and ISO 22301 (business continuity). The new edition of ISO 28000 (notably Clause 4) directly includes recommendations for implementing eight security management principles that are conceptually aligned with and derived from the fundamental principles of ISO 31000 [5]. At the same time, Clause 8 of ISO 28000, which governs the development of risk prevention strategies, procedures, and plans, demonstrates full consistency with the business continuity requirements set out in ISO 22301 [3]. This deeply integrated approach enables critical infrastructure enterprises not only to establish fortified lines of defense for protecting physical assets, but also to develop highly resilient and viable disaster management strategies. As a result, organizations can remain operationally capable and economically sustainable even under the pressure of the most severe conditions, such as large-scale armed conflicts or global pandemics [14].

At the core of the practical implementation of ISO 28000 and the related ISO 28001 guidance lies a strictly formalized and structured process for assessing supply chain security risks. The methodology of the standard does not allow reliance on intuition; instead, it requires mathematical and logical justification. Within this framework, risk is conceptually defined as a mathematical function of the probability of realization of a specific threat and the severity of its potential consequences [15]:

$$R = P(T/V) \cdot C \qquad (1)$$

where R denotes the level of risk; $P(T/V)$ represents the probability of realization of threat T, taking into account the existing system vulnerability V; C denotes the severity of consequences resulting from the realization of this threat.

According to the detailed methodology outlined in ISO 28001, the risk management process is cyclical and consists of eight mandatory stages, each of which is accompanied by the preparation of appropriate documentation [11]. At the first stage, the scope is defined and the supply chain is mapped. This makes it possible to clearly delineate the boundaries of the security management system, identify all participants in the chain (suppliers, carriers, warehouse operators, customs brokers, and end recipients), and visualize all material, information, and financial flows between them.

At the second stage, assets and sources of threats are identified. A comprehensive register of physical assets (vehicles, warehouses), information assets (customer databases, routing documents), personnel, and supporting infrastructure is compiled. In parallel, a threat catalogue is developed, ranging from traditional natural hazards to hybrid attacks, terrorism, and organized crime [16].

At the third stage, vulnerability analysis and incident probability assessment are performed. These procedures are based on internal supply chain security audits aimed at identifying weaknesses in the existing control architecture [17]. Each vulnerability is correlated with the set of threats to calculate the probability parameter.

The fourth stage involves consequence analysis, which determines the potential scale of the destructive impact of an incident on business process continuity, financial stability, brand reputation, and – most critically for critical infrastructure – risks to human life and health [17].

At the fifth stage, a security plan is developed and risks are directly treated. Based on a prioritization matrix, management decides for each threat whether to avoid the risk (e.g., rerouting to bypass a hazardous area), mitigate it (through countermeasures such as enhanced video surveillance or cybersecurity), transfer it (by insuring cargo or outsourcing transportation to a certified contractor), or accept it if protection costs exceed potential losses [18].

As the risk management process is cyclical, the fifth stage is followed by implementation, monitoring, effectiveness assessment, and continual improvement, ensuring full closure of the cycle in accordance with the ISO 28001 methodology. At the sixth stage, approved countermeasures (route changes, strengthened physical security, cybersecurity measures, personnel training, etc.) are integrated into daily supply chain operations.

At the seventh stage, the effectiveness of countermeasures and the overall security process is evaluated and monitored. In the event of deviations or changes in the external environment (emerging threats, supply chain modifications, regulatory changes), corrective and preventive actions are activated, with particular attention to the protection of security-related information and response to actual incidents.

At the eighth stage (continuation/repetition of the process), the cycle restarts from the first stage: the scope is reviewed, supply chain mapping is updated, and a new risk assessment iteration is initiated. In this way, the principle of continual improvement embedded in the PDCA (Plan–Do–Check–Act) model is implemented, forming the basis of the supply chain security management system in accordance with ISO 28001.

To enhance the effectiveness of supply chain security management systems of critical infrastructure facilities, an improved logistics risk management process is proposed through the implementation of the requirements of ISO 28000:2022, with integration of the principles of ISO 31000:2018 and ISO/IEC 27001:2022, as well as mandatory management of artificial intelligence risks in accordance with ISO/IEC 42001:2023. The process retains an eight-stage structure with a mandatory element of communication and consultation at all stages, as well as explicit consideration of information assets and AI systems.

At the first stage, in addition to defining the scope and mapping the supply chain, the organizational context is analyzed in accordance with ISO 31000:2018 (Clause 6.3), using AI tools, particularly Graph Neural Networks (GNNs) – to automatically identify hidden dependencies within the supply chain. Consequently, this stage also includes a preliminary assessment of AI-related risks (data inaccuracy, bias, information leakage) in accordance with ISO/IEC 27001:2022 and ISO/IEC 42001:2023.

At the second stage, in addition to identifying assets and sources of threats and compiling a comprehensive register of physical assets (vehicles, warehouses), information assets (customer databases, routing documents), personnel, and supporting infrastructure, an extended threat catalogue is developed. This catalogue ranges from traditional natural hazards to hybrid attacks, terrorism, and organized crime, with mandatory consideration of specific AI-related threats (model inversion, supply-chain attacks on AI service providers). Identification is carried out using AI tools, including Large Language Models (LLMs) for NLP analysis, in accordance with ISO/IEC 27001:2022 (Clause 6.1.2) and ISO/IEC 42001:2023.

At the third stage, in addition to vulnerability analysis and incident probability assessment based on internal supply chain security audits, AI is used to forecast the likelihood of hazardous events. Simultaneously, AI-related risks are assessed in accordance with ISO 31000:2018 (Risk Analysis), ISO/IEC 27001:2022, and ISO/IEC 42001:2023.

At the fourth stage, alongside consequence analysis, impacts on information security (including AI model data leakage) and ethical and social risks of AI application are assessed. AI is also used to simulate incident consequences in accordance with ISO 31000:2018 (Risk Evaluation) and ISO/IEC 42001:2023.

At the fifth stage, in addition to developing security plans and direct risk treatment, AI is applied to validate the justification and effectiveness of specific countermeasures. For AI-related threats, countermeasures from Annex A of ISO/IEC 27001:2022 (supplier controls, specific contractual arrangements) are applied, taking into account the requirements of ISO/IEC 42001:2023.

At the sixth stage, alongside the implementation of countermeasures, AI is used for personnel training in the safe use of technologies, testing model robustness against attacks, and integrating KPIs for AI controls (ISO/IEC 27001:2022, Annex A.6.3; ISO/IEC 42001:2023).

At the seventh stage, in addition to evaluating the effectiveness of countermeasures and monitoring, AI is applied for real-time monitoring. When deviations are detected, corrective actions are activated and

documented within the information security management system in accordance with ISO 31000:2018, ISO/IEC 27001:2022 (Clause 9), and ISO/IEC 42001:2023.

At the eighth stage, in addition to repeating the process from the first stage as part of continual improvement, the evolution of AI technologies, emergence of new threats, and changes in the external environment are considered in accordance with ISO 31000:2018 (Clause 6.6), ISO/IEC 27001:2022 (Clause 10), and ISO/IEC 42001:2023, ensuring full closure of the PDCA cycle within a unified integrated management system.

Table 2 presents the differences between the traditional and the proposed logistics risk management approaches.

It should be noted that at the third stage enterprises face specific machine-learning-related threats that require dedicated response tools. Such threats include:

1. Data poisoning – malicious, covert modification of training datasets used by logistics AI, leading over time to distorted forecasts of port terminal load or required pharmaceutical inventory levels.
2. Model drift – natural or induced degradation of algorithm accuracy due to changes in real-world conditions, which is particularly critical in wartime, when established logistics routes are disrupted while algorithms continue to generate outdated solutions.
3. Adversarial manipulation – generation of specific digital noise to deceive computer vision systems responsible for automated access control of vehicles to critical infrastructure facilities.

Table 2. Differences between traditional and proposed logistics risk management approaches

Stage	Traditional Management (ISO 28001)	Proposed Enhanced Management (Integration of ISO 31000, ISO/IEC 27001, and AI)
1	Definition of scope and supply chain mapping	Additionally: consideration of organizational context (ISO 31000, Clause 6.3); use of AI for automated supply chain mapping with preliminary assessment of AI-related risks (ISO/IEC 27001)
2	Identification of assets and sources of threats; register of physical and information assets and threat catalogue	Additionally: inclusion of AI models and datasets in the asset register; expansion of the threat catalogue to include specific AI-related threats
3	Vulnerability analysis and probability assessment based on internal audits	Additionally: use of AI for anomaly detection and scenario modeling; mandatory assessment of AI risks (ISO 31000 + ISO/IEC 27001 + ISO/IEC 42001)
4	Consequence analysis of incidents (business, finance, reputation, human life)	Additionally: assessment of information security impacts and ethical/social AI risks; use of AI for consequence simulation (ISO 31000, Risk Evaluation)
5	Development of security plans and risk treatment (avoid, mitigate, transfer, accept)	Additionally: AI-specific countermeasures from Annex A of ISO/IEC 27001; full integration with ISO 31000 (Risk Treatment)
6	Implementation of countermeasures with defined timelines and responsibilities	Additionally: integration of AI systems with KPIs; mandatory personnel training and testing of AI models for robustness (ISO/IEC 27001, Annex A.6.3)
7	Effectiveness evaluation and monitoring (audits, KPIs, incident analysis)	Additionally: use of AI for real-time monitoring; documentation within the information security management system (ISO 31000 + ISO/IEC 27001, Clause 9)
8	Cycle repetition (continual improvement)	Additionally: consideration of AI technology evolution; full closure of the PDCA cycle within an integrated management system (ISO 31000, Clause 6.6; ISO/IEC 27001, Clause 10)

To mitigate these cyber-physical threats, the proposed model requires that identified risks be transferred into a strictly defined framework of contractual obligations. Organizations should include uncompromising requirements in service level agreements (SLAs) regarding incident notification within specified timeframes, diversification of software code supply sources, and mandatory provision of software specifications. Such specifications act as a “software bill of ingredients,” enabling security specialists to

rapidly identify vulnerabilities (e.g., outdated code libraries) in third-party components that are invisibly embedded in critical logistics systems [2].

The specificity of logistics risk management for critical infrastructure enterprises is shaped under the pressure of full-scale military aggression. The scale of daily destruction requires businesses not merely situational adaptation of existing systems, but a fundamental rethinking of the very philosophy of national resilience, which makes the principles of ISO 28000 vitally necessary. As an unavoidable response to these challenges, the expert community and public institutions have conceptually identified physical decentralization as the primary instrument for national survival.

DISCUSSION OF RESEARCH RESULTS

The evolution of theoretical approaches and practical instruments for logistics risk management at critical infrastructure enterprises demonstrates a fundamental shift in the paradigm of global corporate governance. The current stage, formalized by the provisions of ISO 28000:2022, definitively moves security issues beyond the narrow context of physical perimeter protection and cargo escort to the level of strategic, integrated organizational resilience [19]. Ensuring the viability of supply chains is no longer the exclusive prerogative of security services; rather, it requires seamless and deep integration of risk identification and prevention processes within quality management systems, environmental monitoring, cybersecurity of information networks, and business continuity protocols under a unified Integrated Management System (IMS) model [20].

In the logistics industry, particularly at the stage of choosing a certification strategy, enterprise management often faces the question of whether to adopt the systemic standard ISO 28000 or to rely on narrowly specialized sectoral standards such as TAPA (Transported Asset Protection Association) or the U.S. program C-TPAT (Customs-Trade Partnership Against Terrorism). A comprehensive comparative analysis of these systems indicates their operational complementarity while simultaneously revealing fundamental differences in their strategic scope and application philosophy (Table 3).

Table 3. Comparative analysis of ISO 28000 and narrowly specialized sectoral standards

Characteristic	ISO 28000:2022	TAPA (FSR/TSR)	C-TPAT
Primary focus	Comprehensive security and resilience management system for the organization [19]	Prevention of asset losses and theft [21]	Customs security and counter-terrorism protection in supply chains [20]
Scope of application	Global; applicable to all types of risks (physical, cyber, operational, financial) and all types of organizations [19]	Specific; focused on physical security of warehouse facilities (FSR) and in-transit cargo transportation (TSR) [19]	Geographically oriented primarily toward imports to the United States and international trade with U.S. partners [20]
Methodology	Process-oriented (PDCA); requires risk assessment and involvement of top management [19]	Oriented toward strict physical security standards (specifications for walls, locks, cameras, alarm systems) [21]	Oriented toward partnership with customs authorities and compliance with partner validation requirements [20]

TAPA standards are highly effective in establishing minimum acceptable physical security barriers, such as protection of walls and roofs, alarm system configuration, access control to warehouse facilities, and in-transit operations [19]. However, their focus is strictly limited to counteracting criminal encroachments on cargo. C-TPAT, in turn, concentrates on the specifics of customs control [20].

In contrast to these specialized instruments, ISO 28000 offers a global and comprehensive approach. It addresses not only theft prevention but also a far broader spectrum of threats, including cyberattacks on routing systems, insider sabotage, financial fraud, information security risks, consequences of natural disasters, and the management of relationships with all stakeholders without exception [21]. Successful certification under ISO 28000 requires a systemic approach and strong leadership commitment from top management, which makes this standard an indispensable foundation for the strategic management of critical infrastructure enterprises. At the same time, TAPA standards can effectively serve as operational-level tools – specific procedural controls implemented within the broader ISO 28000 architecture to meet targeted protection requirements of individual logistics hubs [22].

The proposed logistics risk management structure corresponds to the modern paradigm of cyber-physical security. Under conditions of total digitalization, critical infrastructure enterprises must implement new models of corporate AI risk governance that take into account the stringent requirements of the European NIS2 and CER directives. Logistics companies are required to fundamentally revise contractual relationships by introducing uncompromising cybersecurity hygiene requirements into service level agreements (SLAs) with transport service providers, software developers, and IoT equipment vendors. The use of software specifications, such as Software Bills of Materials (SBOMs), and regular independent audits of routing algorithms should become routine verification procedures to prevent data-poisoning attacks. Ensuring the resilience of critical infrastructure supply chains is not a static condition achieved by certification, but a permanent, complex, iterative process requiring the engagement of the full intellectual and resource potential of enterprises. Only through the synergistic combination of the rigorous, internationally proven ISO 28000 risk management methodology, breakthrough technological innovations, and unprecedented strategic flexibility can a national logistics system be built that is capable not only of absorbing the devastating shocks of the ongoing war, but also of transforming into a powerful and reliable driver of sustainable long-term macroeconomic recovery.

For Ukraine, which has found itself on the front line of confrontation between global systems, the implementation of the requirements and guidelines of the ISO 28000 series is no longer a matter of reputation or competitive advantage – it has acquired an existential significance for the survival of the logistics system, particularly with regard to critical infrastructure facilities. Given the catastrophic scale of physical destruction of transport and energy infrastructure, estimated at tens of billions of dollars, and considering the systemic nature of hostile attacks on vital logistics nodes, outdated centralized management models have demonstrated their fatal vulnerability. Based on a detailed analysis of the evolution of standards, the latest European directives, and the specific conditions of the current wartime context, it is possible to formulate a set of strategic recommendations for managers of critical infrastructure enterprises and governmental institutions.

The wartime experience has demonstrated the necessity of scaling unique mechanisms of public–private partnership in the defense sector. Ensuring the security of strategic supply chains under current conditions has ceased to be an exclusive function of the state. The formation of joint investment funds for the development of “smart” logistics, co-financing the deployment of local electronic warfare and air defense systems for commercial facilities, and the creation of redundant, protected communication lines together form an innovative hybrid security shield.

There is also a critical need for the urgent modernization of the national regulatory and legal framework. Governmental standardization bodies must immediately harmonize the outdated DSTU ISO 28000:2008 with the provisions of the current global standard ISO 28000:2022. This is not merely a formal procedure, but the establishment of a foundation that will enable Ukrainian businesses to integrate the concept of *resilience* and communicate in a common language with international partners, insurance companies, and European investment funds. In turn, this will serve as a catalyst for accelerated adaptation of more than eighty unimplemented EU transport directives, opening critically needed access to billions of euros in financial resources within the framework of the European TEN-T programme.

CONCLUSIONS

The logistics risk management process within supply chain security management systems of critical infrastructure facilities has been improved through the implementation of the requirements of ISO 28000:2022. The proposed approach differs from existing ones by integrating the requirements of ISO 31000:2018 and ISO/IEC 27001:2022, with mandatory consideration of artificial intelligence risks in accordance with ISO/IEC 42001.

The enhanced logistics risk management process includes context definition and supply chain mapping with automated application of AI tools and preliminary assessment of AI-related risks; identification of assets and sources of threats with the inclusion of AI models and datasets; vulnerability analysis and probability assessment using AI for anomaly detection; consequence analysis incorporating the assessment of ethical and social AI risks; application of AI for scenario simulation; development of security plans and risk treatment with integration of specific AI countermeasures; and continuous improvement taking into account the evolution of AI technologies.

Under conditions of hybrid threats and rapid digitalization, reactive approaches–focused on mitigating consequences after an incident–prove to be insufficiently effective. Resilience can be achieved only through proactive management, including continuous monitoring, AI-based risk forecasting, regular simulations, and systematic control. In this context, the use of artificial intelligence may act both as a source of risk and as a

powerful tool for enhancing resilience, particularly through real-time anomaly detection and scenario modeling.

REFERENCES

1. Akinyeye, O., Odutola, A. A., & Badejo, D. (2024). Assessing the impact of ISO 28000:2022 security management systems on supply chain resilience and risk mitigation. *International Journal of Management, Social Sciences, Peace and Conflict Studies*, 7(1). https://www.ijmsspcs.com/index.php/IJMSSPCS/article/view/644

2. Wong, H. I., Sorooshian, S., & Hasan, M. (2019). Benefits that attract industry to implement ISO 28000 to secure supply chain. *TEM Journal*, 8(1), 119–124. https://doi.org/10.18421/TEM81-17

3. Parlov, N., Akrap, G., & Esterhajer, J. (2025). Supply chain security and AI risk governance model for critical infrastructure under NIS2, CER, and CRA. *ACIG Journal*, 4(1). https://www.acigjournal.com/Supply-Chain-Security-and-AI-Risk-Governance-Model-for-Critical-Infrastructure-under,211823,0,2.htm

4. Bugayko, D., & Reznik, V. (2025). Comparative analysis of Ukrainian legislation and international norms regulating the formation and management of the logistics system. *International Journal of Transportation Research and Technology*, 2(1), 49–58. https://doi.org/10.71108/transporttech.vm02is01.04

5. Hellberg, R., & Lundmark, M. (2025). Transformation in European defence supply chains as Ukraine conflict fuels demand. *Scandinavian Journal of Military Studies*. https://sjms.nu/articles/10.31374/sjms.303

6. Ekwall, D. (2012). Supply chain security – Threats and solutions. In N. Banaitiene (Ed.). *Risk management – Current issues and challenge*s, 4–7. https://doi.org/10.5772/48365

7. Pan, S., Trentesaux, D., McFarlane, D., Montreuil, B., Ballot, E. & Huang, G. Q. (2021). Digital interoperability in logistics and supply chain management: State-of-the-art and research avenues towards Physical Internet. *Computers in Industry*,128, Article 103435. https://doi.org/10.1016/j.compind.2021.103435

8. Powell, T. C. (2017). Strategy as diligence: Putting behavioral strategy into practice. *California Management Review*, 59(3), 162-190. https://doi.org/10.1177/0008125617707975

9. Steinbach, A. L., Holcomb, T. R., Holmes, R. M., Devers, C. E. & Cannella, A. A. (2017). Top management team incentive heterogeneity, strategic investment behavior, and performance: A contingency theory of incentive alignment. *Strategic Management Journal*, 38(8), 1701–1720. https://doi.org/10.1002/smj.2628

10. Atadoga, A., Osasona, F., Amoo, O.O., Farayola, O.A., Ayinla, B.S. & Abrahams, T.O. (2024). The role of it in enhancing supply chain resilience: a global review. *International Journal of Management & Entrepreneurship Research*, 6(2), 336-351. https://doi.org/10.51594/ijmer.v6i2.774

11. Becker, A., Ng, A. K., McEvoy, D. & Mullett, J. (2018). Implications of climate change for shipping: Ports and supply chains. *WIREs Climate Change*, 9(2), Article e508. https://doi.org/10.1002/wcc.508

12. European Business Association. (2023). Annual Survey of Ukrainian Logistics Sector: Digital Infrastructure and Innovation Needs. https://eba.com.ua

13. Frederico, G. F. (2023). ChatGPT in supply chains: Initial evidence of applications and potential research agenda. *Logistics*, 7(2), Article 26. https://doi.org/10.3390/logistics7020026

14. Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., Lioy, A., López, D., Santos, H., Gonos, A., Silva, A., Soriano, J., & Kalogiannis, G. (2021). Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture. *Sensors*, *21*(18), 6057. https://doi.org/10.3390/s21186057

15. International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/ IEC 27001:2022). [Online]. Available: https://www.iso.org/standard/27001.

16. Mora Lozano, P. E., & Montoya-Torres, J. R. (2024). Global Supply Chains Made Visible through Logistics Security Management. *Logistics*, 8(1), 6. https://doi.org/10.3390/logistics8010006

17. Blos, M.F.; Hoeflich, S.L.; Dias, E.M.; Wee, H.-M. (2016). A note on supply chain risk classification: Discussion and proposal. *Int. J. Prod. Res.*, *53*, 1568–1569.

18.Kalaiarasan, R.; Olhager, J.; Agrawal, T.K.; Wiktorsson, M. (2022). The ABCDE of supply chain visibility: A systematic literature review and framework. *Int. J. Prod. Econ.*, *248*, 108464.

19.E. Glerean. (2025). Fundamentals of secure AI systems with personal data, European Data Protection Board, Support Pool of Experts Programme. [Online]. Available: https://www.edpb.europa.eu/system/files/2025-06/spe-training-onai-and-data-protection-technical_en.pdf.

20.Tyrkalo Y. (2022). Entrepreneurial Risks: Causes, Consequences and Management (Theoretical Aspects). *Path of Science*, 8(1), 3010–3017. http://dx.doi.org/10.22178/pos.78-4

21.Hirna O. B. (2020) Logistics and supply chains: challenges of the COVID-19 pandemic. *Black Sea Economic Studies*, 55–1, 87–93. https://doi.org/10.32843/bses.55-14

22.Skrynkovskyy R., Tyrkalo Y. (2021). Entrepreneurial Risks: Nature, Types, Assessment Methods and Ways to Reduce Them. *Path of Science*, 7(12), 2015–2023. http://dx.doi.org/10.22178/pos.77-11

Цопа В.А., Чеберячко С.І., Дерюгін О.В., Літвінова Я.В., Клименко І.Ю. **Вдосконалення процесу керування логістичними ризиками підприємств критичної інфраструктури**

Ланцюги постачання підприємств критичної інфраструктури в сучасних умовах характеризуються високою складністю, цифровізацією та зростанням рівня гібридних загроз, що обумовлює необхідність переходу від реактивних до проактивних підходів управління логістичними ризиками. Метою статті є вдосконалення процесу керування логістичними ризиками в системах управління безпекою ланцюга постачань об'єктів критичної інфраструктури шляхом імплементації вимог міжнародного стандарту ISO 28000:2022.

У дослідженні застосовано системний аналіз для розгляду ланцюгів постачання як складних взаємопов'язаних екосистем, а також методи математичного та логічного моделювання для формалізації оцінки ризиків як функції ймовірності реалізації загроз та тяжкості їх наслідків. Запропоновано вдосконалений процес керування логістичними ризиками, що базується на інтеграції вимог стандартів ISO 28000:2022, ISO 31000:2018 та ISO/IEC 27001:2022 із обов'язковим урахуванням ризиків, пов'язаних із застосуванням штучного інтелекту відповідно до ISO/IEC 42001.

Вдосконалений процес охоплює визначення контексту та картування ланцюга постачання із використанням інструментів штучного інтелекту, ідентифікацію активів і джерел загроз з урахуванням ШІ-моделей і датасетів, аналіз вразливостей та оцінку ймовірності інцидентів, аналіз наслідків із врахуванням етичних і соціальних ризиків ШІ, сценарне моделювання, розробку планів безпеки та оброблення ризиків, а також безперервне вдосконалення системи з урахуванням еволюції цифрових технологій. Практичне впровадження запропонованого підходу спрямоване на підвищення стійкості ланцюгів постачання об'єктів критичної інфраструктури в умовах динамічних ризиків і прискореної цифровізації.

Ключові слова: ISO 28000, критична інфраструктура, управління логістичними ризиками, стійкість ланцюгів постачання, інтегровані системи управління, кіберфізична конвергенція, децентралізація інфраструктури, безперервність бізнесу.

ЦОПА Віталій Андрійович, доктор технічних наук, професор кафедри менеджменту та економіки, Приватний вищий навчальний заклад «Міжнародний інститут менеджменту (МІМ-Київ)» e-mail: tsopa.v.a@nmu.one, ORCID: 0000-0002-4811-3712.

ЧЕБЕРЯЧКО Сергій Іванович, доктор технічних наук, професор, професор кафедри охорони праці та цивільної безпеки, Національний технічний університет «Дніпровська політехніка», e-mail: cheberiachko.s.i@nmu.one, ORCID: 0000-0003-3281-7157.

ДЕРЮГІН Олег Валентинович, кандидат технічних наук, доцент, доцент кафедри управління на транспорті, Національний технічний університет «Дніпровська політехніка», e-mail: deriuhin.o.v@nmu.one, ORCID: 0000-0002-2456-7664.

ЛІТВІНОВА Яна Володимирівна, кандидат технічних наук, доцент, завідувач кафедри управління на транспорті, Національний технічний університет «Дніпровська політехніка», e-mail: litvinova.ya.v@nmu.one, ORCID: 0000-0003-2806-4076.

КЛИМЕНКО Ірина Юріївна, кандидат технічних наук, доцент, доцент кафедри управління на транспорті, Національний технічний університет «Дніпровська політехніка», e-mail: klymenko.i.yu@nmu.one, ORCID: 0000-0002-6263-0951.

Vitalii TSOPA, Doctor of Technical Sciences, Professor of the Department of Management and Economics, Private Higher Educational Institution "International Management Institute (MIM-Kyiv)", e-mail: tsopa.v.a@nmu.one, ORCID: 0000-0002-4811-3712.

Serhii CHEBERYACHKO, Doctor of Technical Sciences, Professor, Professor of the Department of Labour Safety and Civil Security, Dnipro University of Technology, e-mail: cheberiachko.s.i@nmu.one, ORCID: 0000-0003-3281-7157.

Oleh DERYUGIN, PhD (Technical Sciences), Associate Professor, Associate Professor of the Department of Transport Management, Dnipro University of Technology, e-mail: deriuhin.o.v@nmu.one, ORCID: 0000-0002-2456-7664.

Yana LITVINOVA, PhD (Technical Sciences), Associate Professor, Head of the Department of Transport Management, Dnipro University of Technology, e-mail: litvinova.ya.v@nmu.one, ORCID: 0000-0003-2806-4076.

Iryna KLYMENKO, PhD (Technical Sciences), Associate Professor, Associate Professor of the Department of Transport Management, Dnipro University of Technology, e-mail: klymenko.i.yu@nmu.one, ORCID: 0000-0002-6263-0951.

Дата надходження статті до видання: 25.03.2026
Дата прийняття статті до друку після рецензування: 01.05.2026
https://doi.org/10.36910/p22jya05