ECONOMICS OF DEVELOPMENT

Journal homepage: https://ecdev.com.ua/

ISSN: 1683-1942
E-ISSN: 2304-6155

Vol. 25, No. 1, 2026

UDC 658.7:005.334:502.131.1
DOI: 10.63341/econ/1.2026.29

Serhiy Shevchenko*

PhD in Economics, Associate Professor
Lviv Polytechnic National University
79013, 12 Stepana Bandery Str., Lviv, Ukraine
https://orcid.org/0000-0002-5522-3258

Supply chain security within the sustainable development framework: Global practices and the Ukrainian context

Abstract. The relevance of the study was determined by the growing vulnerability of global supply chains under conditions of armed conflict, geopolitical instability, and increasing risks to sustainable development. The purpose of the research was to systematise approaches to supply chain security and to substantiate its role as a key determinant of sustainable development, taking into account international practices and the Ukrainian context. The methodological framework was based on a systematic analysis of scientific literature, comparative analysis of international security programmes, and synthesis and generalisation methods, which made it possible to identify key patterns, risk factors, and institutional mechanisms of supply chain protection. The study established that supply chain vulnerability was driven not only by external shocks, such as military aggression and infrastructure destruction, but also by internal structural characteristics of modern logistics systems, including extended network configurations and lean inventory strategies. It was determined that effective security was achieved through integrated, risk-oriented and partnership-based models, combining public-private cooperation, advance information exchange, and differentiated control mechanisms. The analysis of international programmes (C-TPAT, FAST, CSI, AMR) demonstrated their effectiveness in enhancing supply chain resilience while maintaining trade efficiency. The Ukrainian case confirmed that large-scale disruptions of transport infrastructure generated systemic economic, social, and environmental consequences, thereby directly affecting sustainable development. It was substantiated that supply chain security functioned as a cross-cutting factor linking economic continuity, social stability, and environmental responsibility. The practical significance of the results lies in their applicability for policymakers, logistics managers, and enterprises in developing adaptive, resilient, and security-oriented supply chain management models in conditions of crisis and post-war recovery

Keywords: transport infrastructure; logistics resilience; risk management; public-private cooperation; infrastructure disruption; international trade; post-war recovery

INTRODUCTION

Contemporary global instability, driven by armed conflicts, geopolitical tensions, and increasing threats to transport infrastructure, has significantly transformed the functioning of supply chains, making them more vulnerable and less predictable. Under such conditions, logistics systems were no longer limited to their traditional operational role but increasingly perform strategic functions related to economic resilience, social stability, and environmental responsibility. The vulnerability of modern supply chains was determined not only by external shocks, such as military aggression and disruptions of transport routes, but also by internal structural characteristics, including extended network configurations, limited inventory buffers, and dependence on critical infrastructure.

Recent studies (2020-2026) indicate a clear shift in supply chain management from efficiency-oriented models toward resilience- and security-oriented approaches. O. Aigbogun *et al*. (2022) conceptualise supply chain resilience as a dynamic organisational capability that allows firms to anticipate, absorb, and recover from disruptions,

Article's History: Received: 13.11.2025; Revised: 27.02.2026; Accepted: 26.03.2026; Published: 09.04.2026

Suggested Citation:

Shevchenko, S. (2026). Supply chain security within the sustainable development framework: Global practices and the Ukrainian context. *Economics of Development*, 25(1), 29-40. doi: 10.63341/econ/1.2026.29.

*Corresponding author

thereby maintaining operational continuity. P.E. Mora Lozano & J.R. Montoya-Torres (2024), using modelling and optimisation methods, demonstrate that incorporating resilience considerations into supply chain design improves adaptability and system performance under uncertainty. Similarly, X. Ren *et al*. (2024) provided empirical and analytical evidence that resilience-oriented strategies enhance robustness and reduce vulnerability to disruption. Within this paradigm, supply chain security is increasingly understood not only as a protective function but also as a strategic element of sustainable development. At the same time, contemporary research emphasises the systemic and interconnected nature of supply chain disruptions. M. Herburger *et al*. (2024) showed that disruptions can propagate across interconnected logistics networks, producing cascading effects that amplify risks across sectors. T. Rahman *et al*. (2022), drawing on evidence from the COVID-19 pandemic, demonstrate that global supply chains are highly sensitive to external shocks due to their interdependence and limited redundancy. These findings highlight the need for integrated approaches that combine risk management, institutional coordination, and digital technologies to strengthen supply chain security. These challenges are particularly evident in Ukraine, where the full-scale war has caused extensive damage to transport infrastructure, disrupted logistics routes, and reduced international trade capacity. According to D. Andrienko *et al*. (2024), analytical assessments indicate significant losses in infrastructure and a decline in export potential, necessitating rapid adaptation of logistics systems. UNCTAD (2024) similarly reports substantial disruptions in trade flows and supply chain stability, emphasising the importance of flexible and adaptive logistics strategies under extreme conditions. The disruption of logistics systems in Ukraine is further exacerbated by inconsistencies between national regulatory frameworks and international supply chain management standards. D. Bugayko & V. Reznik (2025), based on institutional analysis, identify regulatory gaps that hinder effective integration into global supply chains and complicate the implementation of modern logistics practices. International experience suggests that effective supply chain security depends on the integration of institutional trust mechanisms and resilience-oriented logistics systems. T. Karavayev *et al*. (2022) find that cooperation between customs authorities and businesses improves transparency and reduces risks in cross-border supply chains. L. Lebedeva & D. Shkuropadska (2024) show that the development of resilient transport and logistics systems, combined with coordinated governance, is essential for maintaining supply chain stability in both developed and transition economies.

Despite the growing body of research, insufficient attention is still paid to the complex analysis supply chain security as a component of sustainable development, particularly in the context of armed conflicts. This creates a research gap that necessitates a systematic examination of supply chain security integrating international experience with the specific challenges faced by Ukraine. The purpose of this article was to systematise approaches to supply chain security under conditions of global instability and to substantiate its role as a key determinant of sustainable development, taking into account international practices and the Ukrainian context.

MATERIALS AND METHODS

The research was based on a comprehensive methodological framework that combines general scientific and specialised methods aimed at analysing supply chain security within the sustainable development framework, with particular attention to global practices and the Ukrainian context. The applied methodology ensures a systematic and reproducible examination of the research problem and allows for the integration of theoretical, analytical, and contextual approaches.

The primary method employed in the study was a systematic analysis of scientific literature, which served as the foundation for examining existing theoretical approaches to supply chain security, logistics resilience, risk management, and sustainable development. Academic publications were selected based on the following criteria: relevance to supply chain security, logistics resilience, and sustainable development; publication within the period 2020-2026; inclusion in recognised scientific databases (Scopus, Web of Science, and peer-reviewed journals); and a focus on risk management, resilience, and security in both global and conflict-affected contexts. In addition, policy reports, and analytical studies by international organisations were reviewed to identify dominant concepts, methodological approaches, and research gaps. The information base of the study was also formed by analytical reports of international organisations (in particular, UNCTAD) and statistical data on infrastructure losses and economic damage provided by the KSE Institute, which were used for empirical validation of theoretical findings. The literature analysis enabled the formulation of the conceptual framework of the study and ensured the consistency of the research with contemporary academic discourse.

Methods of synthesis and generalisation were applied to integrate and systematise findings from diverse sources. Through synthesis, individual elements related to supply chain security, sustainability, and resilience were combined into a coherent analytical model, while generalisation allowed for the identification of common patterns, principles, and trends across different geographical and institutional contexts. These methods facilitated the development of a holistic understanding of supply chain security as a multidimensional phenomenon embedded in economic, social, and environmental dimensions of sustainable development. The abstraction method was used to highlight the essential characteristics and key determinants of supply chain security, enabling the isolation of critical factors influencing logistics stability under conditions of global instability and armed conflict. Accordingly, specific security tools (such as satellite tracking systems, CCTV, or access control mechanisms) were considered as functional categories of monitoring, control, and risk mitigation rather than analysed as isolated technical instruments.

A comparative analysis was employed to examine international practices in supply chain security and to assess their applicability to the Ukrainian context. This method enabled the identification of similarities and differences in institutional arrangements, risk management approaches, and resilience-building strategies across countries, as well as the evaluation of their potential adaptation to national conditions affected by war-related disruptions. The United States was selected as a reference case due to its advanced

institutionalised supply chain security frameworks (including C-TPAT, FAST, CSI, and AMR), long-term implementation experience, and global influence on trade security standards. This case is considered representative of risk-oriented and partnership-based logistics governance models and therefore relevant for adaptation in high-risk environments such as Ukraine.

In addition, elements of the case study method were applied, focusing on Ukraine as a country experiencing large-scale disruptions of supply chains due to armed conflict. This approach enabled an in-depth analysis of real-world processes, including infrastructure damage, transformation of logistics routes, and changes in transport modalities. In addition, contextual and empirical analysis was applied to assess the impact of armed conflict on Ukraine's transport and logistics systems. Secondary data from official statistics, analytical reports, and sectoral assessments were used to evaluate infrastructure losses, changes in transport modalities, and disruptions in supply chain functioning. This included the analysis of statistical and analytical reports of the KSE Institute and UNCTAD, which provided quantitative evidence of infrastructure losses and global logistics trends. This approach allowed for the validation of theoretical assumptions through real-world observations without relying on primary data collection. Overall, the combination of the above methods ensured a comprehensive assessment of supply chain security within the sustainable development framework. The applied methodology provides transparency regarding the research process and offers sufficient detail to enable replication or extension of the study by other researchers using similar materials and analytical approaches.

RESULTS AND DISCUSSION

Contemporary threats to global security have a profound impact on the movement and functioning of logistics systems, particularly in high-risk regions. Armed conflicts lead to the destruction of infrastructure, restrictions on transport routes, and rising operational costs, which significantly complicate the distribution of goods and resources. In areas of active hostilities, supply chains become unstable, requiring continuous adaptation and the use of alternative routes and supply mechanisms. As a result, delivery speed declines, the risk of losses increases, and the regularity of supply is disrupted. These disruptions were reflected in measurable operational consequences, including increased delivery lead times, higher transportation costs, reduced reliability of supply schedules, and the necessity to redesign logistics routes. In particular, the shift towards alternative transport corridors and multimodal solutions led to longer logistics chains and additional coordination costs, thereby increasing overall system complexity and reducing efficiency.

Terrorist attacks and crimes against transport assets and property have become a recurrent phenomenon in the modern world. Although the costs associated with disruptions caused by such events are difficult to quantify precisely, they are highly tangible for affected enterprises. The main consequences include managerial time losses, the need to replace damaged assets, interruptions in service provision, increased insurance premiums, legal expenses, and overall organisational destabilisation. The scale and systemic nature of these consequences became particularly evident following the terrorist attacks on the World Trade Centre in New York and the Pentagon in Washington on September 11, 2001. Since then, logistics security has attracted heightened attention from national governments. One of the immediate responses by the United States government was the introduction of a number of specialised initiatives, including the Customs-Trade Partnership Against Terrorism (C-TPAT), the Free and Secure Trade (FAST) program, the Container Security Initiative (CSI), and the Advanced Manifest Regulations (AMR), commonly known as the "24-hour rule". These measures were aimed at reducing the likelihood of similar attacks in the future.

The analysis indicates that the practical effectiveness of these programmes is manifested through a reduction in customs clearance time, improved predictability of cross-border operations, and lower inspection rates for certified participants. At the same time, their implementation contributes to enhanced transparency and traceability within supply chains, which is critical for reducing security risks and improving coordination among logistics actors. Enhancing supply chain security requires the integration of advanced verification mechanisms and technologies that improve transparency, trust, and coordination among participants (Curado Silveirinha *et al.*, 2025).

Previous studies indicated that terrorist threats are not confined to the territory of a single country, which in turn intensifies concerns regarding the vulnerability of supply chains at the global level. Consequently, it is essential to study and adopt international best practices, as well as to improve and develop new risk management instruments within the distribution systems of Ukrainian enterprises. Given that the United States of America is the world's largest economy and was directly affected by the terrorist attacks of September 11, 2001, it is appropriate to examine in greater detail the measures implemented by this country to prevent subsequent threats and to consider this market as a reference point for the development of general security frameworks. The analysis showed that regulatory requirements in the field of security are subject to continuous improvement and refinement. In contemporary conditions, partnership between customs authorities and the business sector represents a key factor in ensuring efficient logistics, as it enables the optimisation of customs procedures, reduction of cargo transit time, and mitigation of disruptions within supply chains. Through information sharing and coordinated actions, the reliability of logistics processes and the stability of international trade are significantly enhanced.

Cooperation between customs authorities and business entities is also one of the critical factors in preventing terrorist threats and strengthening the security of international trade. Joint efforts by public institutions and the private sector facilitate the timely identification of potential risks, the exchange of relevant information, and the implementation of coordinated preventive measures. Businesses, as active participants in logistics processes, contribute to greater supply chain transparency, while customs authorities ensure control, risk analysis, and border protection. This approach forms a comprehensive security system that reduces the likelihood of trade channels being exploited for terrorist purposes. C-TPAT is a voluntary international supply chain security program initiated

by the U.S. Customs and Border Protection in the aftermath of the 2001 terrorist attacks. Its primary objective is to strengthen border security and international trade through structured cooperation between government authorities and the private sector. Program participants commit to implementing security standards and conducting risk assessments within their supply chains, which enables the identification of vulnerabilities and the prevention of their misuse for illicit activities.

The main goal of the program is to establish a framework for close and systematic cooperation among U.S. importers, carriers, and international exporters supplying goods to the United States. Participants are required to conduct comprehensive assessments of supply chain security, submit a supply chain security profile questionnaire to the competent authority, develop and implement security enhancement programs, and communicate C-TPAT requirements to other companies within their respective supply chains. C-TPAT operates according to the principle of "trust but verify". Companies undergo risk assessments, submit applications, develop security profiles, and implement requirements related to the protection of cargo, equipment, and personnel. Following certification, participants receive tangible benefits in customs clearance procedures, including accelerated cargo processing and a reduced number of inspections (U.S. Customs and Border Protection [CBP], n.d.).

C-TPAT participants are granted a range of significant advantages, such as expedited customs clearance, fewer inspections, assignment of a dedicated supply chain security specialist, access to the C-TPAT partner list, the possibility of using simplified accounting procedures, an emphasis on self-regulation, and access to designated FAST lanes at the borders with Canada and Mexico. The examination of international supply chain security initiatives demonstrates that their effectiveness is primarily determined not by individual control measures but by the integration of risk-based management, advance information exchange, and partnership mechanisms (Mora Lozano & Montoya-Torres, 2024). Programs such as C-TPAT and FAST illustrate that differentiated treatment of low-risk operators allows security objectives to be achieved without creating excessive barriers to trade. The results suggest that security-oriented partnership models simultaneously enhance control, reduce transaction costs, and increase the reliability of logistics flows, thereby strengthening overall supply chain resilience. These programmes also contribute to environmental sustainability by reducing idle time at borders, optimising transport routes, and lowering fuel consumption and emissions. However, under wartime conditions, forced rerouting of logistics flows may offset these benefits, increasing environmental pressure.

In Ukraine, C-TPAT does not operate as a national government program. However, Ukrainian companies that conduct business in the United States or participate in global supply chains may become C-TPAT participants by meeting the relevant requirements of U.S. Customs and Border Protection and successfully completing the certification process. Participation enables such companies to obtain tangible logistical benefits, including expedited customs clearance in the United States, provided that they comply with the established criteria and security standards. Furthermore, C-TPAT is linked to other international supply chain security standards, such as the European Authorised Economic Operator (AEO) system, through mutual recognition mechanisms. These arrangements contribute to strengthening partnerships between customs authorities and the business sector across different countries, including Ukraine, and facilitate greater interoperability of security regimes in international trade. Under conditions of full-scale war and heightened security risks, modern international mechanisms for protecting supply chains acquire particular significance for Ukraine. Over more than a decade of implementation, C-TPAT has demonstrated an effective partnership-based model of cooperation between public authorities and the private sector, contributing to enhanced logistics resilience, reduced risks of illicit activities, and increased trust among participants in international trade. For Ukrainian companies, participation in C-TPAT represents not only a tool for gaining practical logistical advantages but also an important step toward integration into global security and trade standards. In the longer term, the experience of this program may serve as a valuable foundation for the development of national initiatives in the field of logistics security, which is critically important for economic recovery and the strengthening of Ukraine's position in global markets.

With reference to Ukraine, the results indicated that the absence of nationally embedded supply chain security frameworks comparable to international partnership-based models increases exposure to systemic logistics risks. While Ukrainian companies may individually participate in international security programs, the lack of coordinated national mechanisms limits the scalability of security benefits across supply chains. This finding highlights a structural gap between international logistics security practices and national institutional capacity, which directly affects the resilience and sustainability of Ukraine's supply chains under wartime conditions. A comparative analysis revealed significant structural differences between international supply chain security models and the Ukrainian logistics system. In particular, advanced economies such as the United States rely on institutionalised public-private partnership frameworks, risk-based customs procedures, and certified trusted operator programmes, which ensure both high security and operational efficiency. In contrast, the Ukrainian system remains characterised by fragmented institutional coordination, limited implementation of risk-based approaches, and the absence of fully developed national security programmes. These differences indicate a structural gap that constrains the scalability of security mechanisms and reduces the overall resilience of supply chains under wartime conditions.

To better understand the structural differences in supply chain security approaches, a comparative analysis of institutional, procedural, and technological dimensions was conducted. The comparison focuses on established international practices, particularly the United States model based on public-private partnerships and risk-based management systems, and contrasts them with the current Ukrainian context. This analytical framework allows for the identification of systemic gaps and potential directions for improving supply chain resilience and security (World Customs Organisation, 2021; Mora Lozano & Montoya-Torres, 2024).

A comparative analysis of institutional models of supply chain security in the United States and Ukraine, including differences in risk management, customs procedures, and trust mechanisms, is presented in Table 1.

Table 1. Comparative analysis of supply chain security models

Dimension	USA (C-TPAT / FAST)	Ukraine
Institutional model	Public-private partnership	Fragmented
Risk management	Risk-based	Reactive
Customs procedures	Simplified	Complex
Trust mechanisms	Certified operators	Limited
Digitalisation	High	Partial

Source: compiled by the author based on World Customs Organisation (2021), P.E. Mora Lozano & J.R. Montoya-Torres (2024), H. Zheng *et al*. (2024)

As shown in Table 1, the U.S. model demonstrates a high level of institutional integration, relying on structured public-private partnerships, certified operator programmes, and advanced digital systems. International studies indicate that supply chain security is closely associated with the integration of institutional trust mechanisms and resilience-oriented logistics systems. In particular, the Authorised Economic Operator (AEO) programme enhances cooperation between customs authorities and businesses, while the resilience of transport logistics systems has become a key factor in ensuring the stability of supply chains in the EU and Ukraine (Karavayev *et al.*, 2022; Lebedeva & Shkuropadska, 2024). In contrast, Ukraine's supply chain security framework remains fragmented, with limited coordination between stakeholders and a predominance of reactive risk management approaches. Supply chain decision-making under uncertainty requires the application of structured risk assessment models capable of capturing complex interdependencies between system components (Rahman *et al.*, 2022).

At the same time, the effectiveness of supply chains is often constrained by structural barriers. Maritime supply chains are significantly affected by a wide range of barriers, particularly infrastructural and regulatory constraints, which play a critical role in determining their efficiency and performance (Kashav *et al.*, 2022). The most significant differences are observed in the areas of risk management and trust-based mechanisms. Recent research highlights that resilience and sustainability in supply chains are closely interconnected and should be addressed simultaneously within risk management frameworks (Meng *et al.*, 2025). While the U.S. system is built on proactive risk assessment and the recognition of trusted economic operators, Ukraine still lacks a fully institutionalised system of certification and mutual trust between business and regulatory authorities (World Customs Organisation, 2022; Zheng *et al.*, 2024).

Furthermore, the level of digitalisation plays a critical role in enhancing transparency and predictability in supply chain operations. The partial implementation of digital tools in Ukraine limits the effectiveness of security controls and increases operational uncertainty, particularly under crisis conditions (Ren *et al.*, 2024). Cybersecurity has become a critical component of supply chain resilience, as increasing digitalisation expands the range and complexity of potential disruptions. These structural differences indicate that strengthening supply chain security in Ukraine requires not only technological modernisation but also institutional transformation, including the development of trust-based frameworks and the integration of international best practices.

In the logistics context, free and secure trade is regarded as a key condition for the effective functioning of global supply chains, where cross-border material flows occur with minimal regulatory barriers while maintaining strict security requirements. Trade liberalisation contributes to the optimisation of logistics processes by reducing customs delays, simplifying border-crossing procedures, harmonising transport and accompanying documentation, and lowering transaction costs in international transportation. At the same time, the security dimension of logistics entails the implementation of standards and technologies aimed at protecting cargo, infrastructure, and information systems, controlling the origin and quality of goods, and preventing smuggling, terrorist threats, and the spread of hazardous materials. Consequently, within logistics systems, free and secure trade emerges as an integrated concept that combines faster and more cost-efficient cargo movement with the assurance of physical, economic, and regulatory protection at all stages of the supply chain.

Under conditions of escalating global challenges, military threats, and the destabilisation of logistics routes, supply chain security has become a critical issue not only for trade stability but also for national economies as a whole. This is particularly relevant for Ukraine, which operates in a high-risk environment and requires the adoption of effective international approaches to protecting logistics processes. One of the most effective instruments that reconciles the interests of the state and the business sector in the context of secure trade is the Free and Secure Trade (FAST) program. Its experience deserves special attention as a reference point for the modernisation of Ukraine's logistics system. FAST is a joint initiative of the customs authorities of the United States, Canada, and Mexico, designed to simplify and accelerate cross-border cargo movements through the prior verification of trusted international trade participants. The program targets businesses that adhere to high security standards within their supply chains, granting participants benefits such as streamlined customs procedures, reduced inspection times, and access to dedicated border lanes.

The practical effectiveness of the FAST initiative is most clearly demonstrated through the analysis of specific cross-border transportation cases, where the combination of advance participant verification and risk-based control mechanisms leads to shorter border clearance times and enhanced predictability of logistics operations. Experience

with FAST in real-world supply chains shows that security requirements, including driver identification, verification of carrier reliability, and compliance with procedural standards, can be integrated into day-to-day operational activities without increasing administrative burdens. Instead, these requirements are transformed into a competitive advantage by reducing idle time, optimising delivery schedules, and stabilising service levels. In this context, illustrative cases provide evidence of FAST's impact on transit times, costs, and the organisation of interactions among logistics stakeholders.

The FAST initiative applies to border crossings between the United States and Canada and Mexico. Its primary objective is to ensure faster and more efficient clearance of cargo for C-TPAT-certified participants at these borders. Certified commercial vehicle drivers participating in C-TPAT are entitled to use designated FAST lanes, which significantly accelerate border-crossing procedures. Overall, the program is aimed at enhancing supply chain security while avoiding unjustified barriers to international trade. Beyond the use of designated lanes, the FAST mechanism is based on the principle of prior selection of "trusted" supply chain participants and the application of risk-oriented control. To benefit from the program, the key parties involved in transportation must typically be approved, including the importer (through participation in C-TPAT), the carrier, and the driver, all of whom undergo reliability checks and comply with established requirements for physical and procedural security. In practical terms, this approach implies strengthened control at the stages of shipment preparation and planning, including standards for cargo protection, facility access, documentation, and traceability, followed by a reduction in border delays due to fewer inspections and faster routine procedures for low-risk shipments.

Within logistics systems, the application of FAST enhances the predictability of cross-border operations and reduces time-related and financial losses associated with vehicle downtime, congestion, and additional administrative costs. This is particularly important for time-sensitive supply chains, such as those operating under just-in-time production models, where the stability of border crossings directly affects inventory levels, fulfilment of contractual obligations, and overall competitiveness. At the same time, the program strengthens the integration of security procedures into logistics management, shaping a model of "secure speed," in which the acceleration of cargo flows is achieved not by reducing control, but by more precisely targeting high-risk movements.

For Ukraine, which is currently operating under wartime conditions, sustained pressure on transport infrastructure, and a critical dependence on foreign economic relations, the principles underlying the FAST program may have strategic significance. Its implementation or adaptation to Ukrainian realities, even in the form of a pilot partnership initiative, could become an important instrument for restoring trust in Ukrainian logistics operators, improving customs administration, and ensuring the security of international cargo flows. Participation in such initiatives also opens additional opportunities for Ukrainian exporters, including faster customs clearance, cost reductions, and simplified cooperation with partners in the United States, Canada, Mexico, and other countries that recognise comparable security standards. In a broader perspective, the development of secure and efficient logistics channels constitutes an integral component of a sustainable development strategy. It encompasses not only economic performance but also environmental responsibility, social resilience, and sound governance. Reliable logistics systems form the foundation of functioning markets, support for small and medium-sised enterprises, humanitarian supply, and investment attraction. Consequently, the integration of FAST principles into Ukraine's logistics management system may serve not only as a mechanism for crisis response but also as a cornerstone for sustainable recovery and long-term growth.

It is also important to highlight other initiatives that contribute to strengthening supply chain security at the international level. Among them, a key role is played by the Container Security Initiative (CSI), which provides the advance screening of potentially high-risk cargo at ports of departure before their arrival in the United States (U.S. Customs and Border Protection, n.d.). This model is based on the use of intelligence data, advanced scanning technologies, and containers equipped with built-in protection mechanisms against unauthorised interference. The CSI framework is complemented by the Secure Freight Initiative (SFI), which expands the technical capabilities of cargo inspection and covers a broad range of major international ports (U.S. Customs and Border Protection, n.d.). Another important instrument is the Advanced Manifest Rule (AMR), which requires carriers and exporters to submit detailed cargo information in advance. This mechanism enables the identification of risks prior to border crossing and helps prevent the unauthorised importation of dangerous or illicit goods.

Such programs not only enhance security in global logistics systems but also contribute to the establishment of new standards of sustainable development, particularly by minimising delays, reducing costs, and ensuring transparency in supply chains. They also promote higher levels of environmental and social responsibility among businesses, as sustainable development encompasses not only economic efficiency but also the safety of logistics processes for people and the environment. As Ukraine continues its integration into global markets, it has strong grounds for adopting best international practices in logistics security and adapting them to national conditions. The implementation of similar approaches or participation in programs such as CSI or AMR, even in the form of pilot initiatives, would enable Ukrainian companies not only to reduce risks but also to enhance their competitiveness and credibility at the global level.

Transport infrastructure has become one of the sectors that has suffered the most significant losses as a result of Russia's full-scale military aggression against Ukraine. In the first weeks of the war, Russian forces carried out massive strikes on aviation infrastructure facilities, primarily airfields that were used not only for military purposes but also for civilian and dual-use (civil-military) operations. Subsequently, railway infrastructure, which plays a system-forming role in the national logistics system, became a major target of sustained attacks. The total losses of Ukraine's transport sector are estimated at approximately USD 38.8 billion in terms of revenue losses, or nearly

USD 19 billion in terms of value-added losses (Andrienko *et al.*, 2024). This figure includes lost revenues of enterprises within the sector, costs associated with the dismantling of destroyed facilities, economic losses resulting from reduced road construction activity, as well as expenditures related to the performance of both civilian and military tasks under martial law.

Since the onset of the full-scale war, rail transport has demonstrated its critical importance in ensuring the economic and humanitarian security of the state. The railway system assumed the primary responsibility for the free evacuation of millions of Ukrainian citizens, as well as a significant number of enterprises from areas of active hostilities. In addition, railway infrastructure ensured the delivery of critically important materials and equipment to frontline regions. In response to this strategic role, railway facilities became priority targets of missile and artillery attacks, resulting in substantial losses, primarily in the form of foregone revenues for JSC Ukrzaliznytsia. The aviation sector began to incur economic losses even before the actual outbreak of active hostilities. On February 12, 2022, leading international insurance companies notified Ukrainian air carriers of the suspension of aircraft insurance due to the high risk of a military invasion. This development posed a serious threat of flight cancellations by international airlines operating to and from Ukraine, prompting the state to declare its readiness to provide additional financial guarantees to support the functioning of the aviation market. Following the escalation of hostilities, Ukraine's airspace was fully closed and air traffic suspended. Simultaneously, Russian forces carried out a series of missile strikes on key airfields with the objective of undermining Ukraine's air defence capabilities. As a result, 19 out of 35 airfields were damaged, including 12 civilians and 7 dual-use (civil-military) facilities, excluding purely military airfields. Some of these sites were subjected to repeated shelling (Andrienko *et al.*, 2024).

After the beginning of the full-scale invasion, all maritime trade routes of Ukraine became inaccessible for both exports and imports, causing significant losses to the national economy. In March 2022 alone, export volumes declined by approximately 50%. In August 2022, following agreements reached between Ukraine, Türkiye, the United Nations, and Russia, the operations of three Ukrainian ports – Odesa, Pivdennyi, and Chornomorsk – were partially unblocked. In 2021, these ports accounted for nearly 70% of Ukraine's foreign trade turnover. Within the framework of the so-called "grain initiative," a total of 19 million tonnes of agricultural products were exported through maritime ports between August 2022 and June 2023. Nevertheless, even during the implementation of this initiative, maritime trade capacity remained constrained, and Russia subsequently began to systematically sabotage the agreements and refused to extend them further. Despite these challenges, Ukraine managed to partially restore maritime navigation unilaterally through the actions of its Defence Forces (UNCTAD, 2024).

Municipal transport infrastructure in regions of active hostilities also suffered extensive destruction. As a result of large-scale attacks on civilian infrastructure, residents of many cities were left without access to public transportation and private vehicles. The most severe losses of municipal assets occurred in the Luhansk and Donetsk regions, as well as in the city of Kharkiv. Estimates indicate that approximately 60% of public transport assets were lost in Donetsk region and more than 70% in Luhansk region, effectively leading to the collapse of passenger transport systems in these areas. A substantial share of privately owned vehicles was also destroyed or damaged (Andrienko *et al.*, 2024). A comparative analysis of institutional approaches to supply chain security in the United States and Ukraine, including differences in risk management, customs procedures, trust mechanisms, and the level of digitalisation, is presented in Table 2.

Table 2. Assessment of losses in Ukraine's transport sector

Types of losses	Revenue losses, USD bn	Value added losses, USD bn
Decline in revenues (road transport)	7.130	3.257
Decline in revenues (rail transport)	6.442	2.943
Decline in revenues (warehousing and storage)	5.666	2.588
Decline in revenues (water transport)	4.313	1.970
Decline in revenues (postal and courier activities)	3.849	1.758
Decline in revenues (urban transport)	1.332	0.608
Decline in revenues (other activities)	0.985	0.450
Costs of dismantling and removal of construction debris	6.763	3.090
Total sector losses	38.814	18.664

Source: D. Andrienko *et al.* (2024)

As shown in Table 2, the US model is characterised by a high level of institutional integration, risk-based management, and active public-private cooperation, whereas the Ukrainian system remains fragmented, with limited implementation of trust mechanisms and a lower level of digitalisation. These differences highlight the need to adapt international best practices to the Ukrainian context, taking into account institutional and operational constraints. The concentration of losses in system-forming logistics segments demonstrates the high level of structural dependence of supply chains on centralised infrastructure. This finding confirmed that insufficient diversification of transport routes and logistics nodes significantly increases systemic vulnerability under crisis conditions. The results indicate that the most significant losses within Ukraine's transport sector are concentrated in segments that perform system-forming logistics functions, particularly rail transport, road freight transport, and warehousing activities. These segments ensured the continuity of material flows between production, distribution, and consumption nodes,

and their disruption generated cascading effects across entire supply chains. The concentration of losses in these areas confirms the high structural vulnerability of logistics systems that rely on centralised infrastructure and limited route diversification. As a result, supply chain security risks increase not only at the operational level but also at the systemic level, undermining predictability, controllability, and resilience of logistics networks.

International experience demonstrates that resilient supply chains are built on the combination of risk-based governance, public-private cooperation, and advanced digital systems (World Customs Organisation, 2022; UNCTAD, 2023). The full-scale war in Ukraine has become an unprecedented example of the systemic destruction of logistics infrastructure. Massive attacks on aviation, rail, and maritime facilities, the blockade of trade routes, and the destruction of urban transport networks have significantly undermined the country's economic security. As noted above, despite extensive damage, rail transport has performed a critical humanitarian and economic function by ensuring the evacuation of millions of citizens and maintaining the supply of essential goods and materials. At the same time, the aviation sector has virtually ceased operations due to the closure of national airspace and the destruction of aerodrome infrastructure. Maritime logistics has faced severe constraints as a result of port blockades, leading to a sharp decline in exports and substantial losses in foreign currency revenues.

The destruction of municipal transport infrastructure in eastern regions of Ukraine has generated not only economic but also profound social consequences, limiting population mobility and access to basic services. In this regard, the war has clearly demonstrated that logistics security is a fundamental prerequisite for social stability and the economic viability of territories. The analysis further reveals that disruptions in transport and logistics infrastructure produce cascading effects across supply chains, undermining their predictability, controllability, and overall security. Losses in core transport and distribution segments indicate structural vulnerability and insufficient diversification of logistics routes, thereby increasing exposure to systemic risks. The classification of supply chain vulnerabilities into infrastructural, organisational, and institutional categories was developed through analytical generalisation and comparative synthesis of findings from the reviewed literature and empirical observations. The analysis revealed that wartime disruptions exposed three interrelated categories of supply chain vulnerabilities: infrastructural, organisational, and institutional. Infrastructural vulnerabilities stem from the physical destruction of transport corridors, logistics hubs, and storage facilities. Organisational vulnerabilities arise from the reduced buffer capacities of supply chains, limited inventory reserves, and dependence on time-sensitive delivery models. Institutional vulnerabilities are reflected in regulatory fragmentation, restricted border access, and limited interoperability between national and international security regimes. Together, these vulnerabilities amplify security risks and constrain the adaptive capacity of supply chains under prolonged crisis conditions.

The destruction of logistics hubs and transport corridors weakens buffer capacities, constrains the redistribution of material flows, and reduces the ability of supply chains to absorb shocks. These dynamics pose direct challenges to supply chain security and hinder sustainable development by amplifying economic uncertainty, social vulnerability, and environmental pressures. Alongside strategic challenges, tactical security measures gain particular importance. Vehicles, distribution centres, and warehousing facilities become potential targets of criminal activity, especially under conditions of weakened control and heightened demand for critical resources. The application of satellite tracking systems, closed-circuit television (CCTV), intrusion alarm systems, and access control mechanisms enhances the transparency and controllability of logistics flows. At the same time, the effectiveness of these measures depends on appropriate organisational arrangements, continuous monitoring, and the professional training of personnel (Ren *et al*., 2024).

Particular attention should be paid to the human factor. Personnel selection, screening, and training procedures constitute a critical component of the security system, as a substantial share of incidents is associated with internal risks rather than external threats. International experience indicates that improving supply chain security is impossible without integrating risk management into the overall corporate governance framework (Herburger *et al*., 2024). A decisive role is played by risk awareness at the senior management level and by the understanding that changes in business strategy directly transform organisational risk profiles. Supply chain vulnerability has increased significantly as a result of the extension and so-called "thinning" of logistics networks between specialised facilities (Rahman *et al*., 2022). Business strategies focused on inventory minimisation, relocation of production to lower-cost countries, and the globalisation of material flows have reduced safety stock levels and heightened system sensitivity to external disruptions.

The findings confirm that post-war recovery cannot be limited to physical reconstruction alone. Instead, it requires the development of integrated supply chain security models that combine resilience, institutional coordination, environmental responsibility, and risk-oriented governance. Research conducted by the Centre for Logistics and Supply Chain Management at Cranfield University (United Kingdom) as early as 2003 demonstrated that the very structure of modern supply chains constitutes an independent source of risk. The study identified four levels of vulnerability, including value creation processes and flows, dependence on assets and infrastructure, organisational and inter-organisational networks, and the external environment. These conclusions have become particularly relevant in the context of pandemics, climate change, and, above all, armed conflicts. Disruptions of supply chains caused by political instability, epidemics, or military aggression are capable of generating catastrophic consequences for individual firms, entire industries, and national economies as a whole (Christopher & Peck, 2004).

In the European Union and North America, logistics security is increasingly interpreted through the lens of sustainable development (Li *et al*., 2026). The economic dimension is reflected in ensuring supply continuity and reducing losses; the social dimension concerns the protection of workers and consumers; while the environmental dimension relates to minimising the negative impacts of

accidents, delays, and inefficient routing on the natural environment. For Ukraine, the application of global best practices and the findings of international research is critically important in the context of post-war recovery. The formation of resilient, diversified, and secure logistics systems should become a priority of both public policy and corporate strategy. The results confirm that supply chain security functions as a cross-cutting determinant of sustainable development under crisis conditions. Disruptions in logistics infrastructure and governance generate economic losses, restrict social mobility and access to essential goods, and increase environmental risks associated with inefficient routing and emergency logistics solutions. Consequently, the security of supply chains emerges not as a secondary operational concern but as a foundational condition for economic resilience, social stability, and environmental responsibility.

Thus, logistics security in wartime conditions extends beyond a purely operational task and transforms into a strategic determinant of sustainable development. The military challenges faced by Ukraine have clearly demonstrated the interdependence between supply chain security, economic resilience, social stability, and environmental responsibility. The integration of international experience, scientific approaches to risk management, and the principles of sustainable development provides the foundation for shaping a new logistics model – resilient, secure, and adaptable to crises. Such a model is capable of supporting long-term recovery and strengthening the competitiveness of Ukraine's economy in the post-war period. In addition, disruptions in logistics systems contribute to increased environmental pressure. The forced extension of transport routes, the use of less efficient alternative modes, and the intensification of emergency logistics operations lead to higher fuel consumption and greenhouse gas emissions. This demonstrated that supply chain security is directly linked not only to economic and social stability but also to environmental sustainability under crisis conditions.

The findings of this study confirm that supply chain security has evolved from an operational concern into a multidimensional strategic function, which is consistent with recent research in the field of logistics and supply chain management. In particular, the results aligned with the conclusions of A. Gurtu & J. Johny (2021), who emphasised that supply chain risk management constitutes a systemic and strategic activity aimed at ensuring the continuity and stability of global logistics networks. The present study extends this perspective by demonstrating that, under conditions of armed conflict, security considerations become central to the functioning of supply chains rather than supplementary.

The identified structural vulnerabilities of supply chains are also consistent with the findings of M. Christopher & H. Peck (2004), who argued that the architecture of supply chains itself represents a significant source of risk. While their research focused primarily on disruptions in relatively stable economic environments, this study confirms that these vulnerabilities are significantly amplified under conditions of war, where infrastructure destruction and institutional constraints intensify systemic instability. The results further support the conclusions of T. Rahman *et al*. (2022), who highlighted the importance of resilience-oriented strategies in mitigating supply chain disruptions. However, unlike previous studies that emphasised resilience primarily in the context of natural disasters or pandemics, the present research demonstrates that wartime conditions require a more integrated approach, combining resilience with security, institutional coordination, and strategic governance.

A significant contribution of this study lies in the integration of supply chain security into the sustainable development framework. This finding is consistent with the research of Y. Borbon-Galvez *et al*. (2025), who demonstrated the complementary relationship between sustainability and resilience. The present study confirms that this relationship becomes particularly pronounced under crisis conditions, where disruptions in logistics systems generate not only economic losses but also social instability and environmental pressures. In addition, the findings correspond with the work of J. Liu *et al*. (2023), who emphasised the importance of adaptability and flexibility in ensuring maritime supply chain resilience. The Ukrainian case analysed in this study illustrates that the ability to rapidly reconfigure logistics routes and utilise alternative transport modes is a critical determinant of supply chain survival under extreme conditions.

At the same time, the results highlight certain differences compared to existing literature. While many studies focus on technological solutions and digitalisation as key drivers of supply chain security (Ren *et al*., 2024), this research demonstrates that under wartime conditions, institutional capacity, infrastructure availability, and international cooperation play a more decisive role than technological advancement alone. Furthermore, the study supports the conclusions of N. Antoniiuk *et al*. (2023), who emphasised the role of financial support and strategic planning in ensuring logistics security. However, the present research expands this perspective by showing that financial mechanisms must be complemented by institutional coordination and international integration in order to be effective in high-risk environments. The comparative analysis of international security programmes (C-TPAT, FAST, CSI, and AMR) confirms the effectiveness of partnership-based models of governance, which is consistent with the SAFE Framework of Standards (World Customs Organisation, 2022). These findings indicate that the integration of public-private cooperation mechanisms significantly enhances both security and efficiency of supply chains. Overall, the results of this study confirm that supply chain security should be considered a core component of sustainable development strategies. The findings demonstrate that economic resilience, social stability, and environmental sustainability are interdependent and cannot be achieved without secure and adaptive logistics systems. This reinforces the need for further research focused on developing integrated models of supply chain security tailored to high-risk and conflict-affected environments.

CONCLUSIONS

The study demonstrated that under conditions of global instability and armed conflict, supply chain security extends beyond its traditional operational role and becomes a strategic determinant of sustainable development. The findings confirmed that supply chain vulnerability is driven

not only by external shocks, such as military aggression and infrastructure destruction, but also by internal structural characteristics, including extended logistics networks, limited diversification of transport routes, and dependence on centralised infrastructure. The analysis showed that disruptions in transport and logistics systems generate cascading effects across supply chains, undermining their predictability, controllability, and resilience. The Ukrainian case provided empirical evidence that large-scale infrastructure damage leads to significant economic losses, reduced social stability, and increased environmental pressure, thereby directly affecting the foundations of sustainable development. The study further established that effective supply chain security is achieved through integrated, risk-oriented, and partnership-based approaches. International practices, including C-TPAT, FAST, CSI, and AMR, demonstrated that public-private cooperation, advance information exchange, and differentiated control mechanisms enhance both security and trade efficiency. From a practical perspective, the results highlight the need to develop national supply chain security frameworks adapted to wartime conditions and aligned with international standards. The formation of resilient, diversified, and risk-aware logistics systems should become a priority of both public policy and corporate strategy in Ukraine's post-war recovery. Future research should focus on the development of integrated models of supply chain security tailored to conflict-affected environments, including the quantitative assessment of resilience and sustainability indicators, the role of digital technologies in logistics risk management, and the evaluation of policy instruments for strengthening institutional coordination and international integration.

ACKNOWLEDGEMENTS
None.

FUNDING
None.

CONFLICT OF INTEREST
None.

REFERENCES
[1] Agricultural Research Centre. (2024). *How Azerbaijan adapts to new technologies in agriculture?* Retrieved from https://atm.gov.az/en/news/1440/how-azerbaijan-adapts-to-new-technologies-in-agric/.
[2] Ahmetoglu, S., Cob, Z.C., & Ali, N.A. (2023). Internet of things adoption in the manufacturing sector: A conceptual model from a multi-theoretical perspective. *Applied Sciences*, 13(6), article number 3856. doi: 10.3390/app13063856.
[3] Albreem, M.A., Sheikh, A.M., Bashir, M.J., & El-Saleh, A.A. (2023). Towards green Internet of Things (IoT) for a sustainable future in Gulf Cooperation Council countries: Current practices, challenges and future prospective. *Wireless Networks*, 29(2), 539-567. doi: 10.1007/s11276-022-03133-3.
[4] Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. *Sensors*, 22(4), article number 1304. doi: 10.3390/s22041304.
[5] Al-Okaily, M., Younis, H., & Al-Okaily, A. (2024). The impact of management practices and industry 4.0 technologies on supply chain sustainability: A systematic review. *Heliyon*, 10(17), article number e36421. doi: 10.1016/j.heliyon.2024.e36421.
[6] Bag, S., & Pretorius, J. (2022). Relationships between industry 4.0, sustainable manufacturing and circular economy: Proposal of a research framework. *International Journal of Organizational Analysis*, 30(4), 864-898. doi: 10.1108/IJOA-04-2020-2120.
[7] Baghirova, N. (2023). *Smart farming for sustainable agriculture in Karabakh*. Baku: ADA University.
[8] Billah, M., Alam, S., Masukujjaman, M., Ali, M., Makhbul, Z., & Salleh, M. (2023). Effects of Internet of Things, supply chain collaboration and ethical sensitivity on sustainable performance: Moderating effect of supply chain dynamism. *Journal of Enterprise Information Management*, 36(5), 1270-1295. doi: 10.1108/JEIM-06-2022-0213.
[9] Caldwell, E. (2023). *Smart villages in Azerbaijan.* Retrieved from https://www.smartrural21.eu/wp-content/uploads/World-Bank-Smart-Villages-Presentation_Erik-Caldwell.pdf.
[10] Cavalieri, A., Reis, J., & Amorim, M. (2022). A conceptual model proposal to assess the effectiveness of IoT in sustainability orientation in manufacturing industry: An environmental and social focus. *Applied Sciences*, 12(11), article number 5661. doi: 10.3390/app12115661.
[11] Cisco. (2024). *Global networking trends report*. Retrieved from https://www.cisco.com/c/dam/global/en_uk/solutions/enterprise-networks/2024-global-networking-trends.pdf.
[12] Ding, S., Tukker, A., & Ward, H. (2023). Opportunities and risks of internet of things (IoT) technologies for circular business models: A literature review. *Journal of Environmental Management*, 336, article number 117662. doi: 10.1016/j.jenvman.2023.117662.
[13] Edquist, H., Goodridge, P., & Haskel, J. (2021). The Internet of Things and economic growth in a panel of countries. *Economics of Innovation and New Technology*, 30(3), 262-283. doi: 10.1080/10438599.2019.1695941.
[14] European Commission. (2024a). *How to master Europe's digital infrastructure needs?* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0081.
[15] European Commission. (2024b). *Internet of Things (rolling plan for ICT standardisation 2024)*. Retrieved from https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/internet-things-rp2024.
[16] Foltean, F.S., & Glovaţchi, B. (2021). Business model innovation for IoT solutions: An exploratory study of strategic factors and expected outcomes. *Amfiteatru Economic*, 23(57), 392-411. doi: 10.24818/EA/2021/57/392.
[17] Fortune Business Insights. (2025). Retrieved from https://surl.li/jkwykk.

[18] Goudarzi, M., Ilager, S., & Buyya, R. (2022). Cloud computing and internet of things: Recent trends and directions. In R. Buyya, L. Garg, G. Fortino & S. Misra (Eds.), *New frontiers in cloud computing and internet of things* (pp. 3-29). Cham: Springer. doi: 10.1007/978-3-031-05528-7_1.
[19] Harikannan, N., Vinodh, S., & Antony, J. (2025). Analysis of the relationship among Industry 4.0 technologies, sustainable manufacturing practices and organizational sustainable performance using structural equation modelling. *The TQM Journal*, 37(1), 42-72. doi: 10.1108/TQM-02-2023-0044.
[20] Huma, Z.E., Latif, S., Ahmad, J., Idrees, Z., Ibrar, A., Zou, Z., Alqahtani, F., & Baothman, F. (2021). A hybrid deep random neural network for cyberattack detection in the industrial internet of things. *IEEE Access*, 9, 55595-55605. doi: 10.1109/ACCESS.2021.3071766.
[21] Huseynova, A., & Mazanova, O. (2023). *The leading role of digital technologies in the development of the smart city concept in Azerbaijan*. doi: 10.2139/ssrn.4800562.
[22] Imamguluyev, R., Hasanova, P., Imanova, T., Poladova, U., Amrahova, A., & Hajibayli, A. (2024). The role of edge computing in 6G-enabled IoT applications. *International Journal of Research Publication and Reviews*, 5(12), 2007-2013. doi: 10.55248/gengpi.5.1224.3523.
[23] International Renewable Energy Agency. (2024). Retrieved from https://www.iea.org/reports/renewables-2024.
[24] ISO/IEC 30141:2024. (2024). *Internet of things (IoT) reference architecture*. Retrieved from https://www.iso.org/standard/88800.html.
[25] Javadpour, A., Sangaiah, A.K., Zhang, W., Vidyarthi, A., & Ahmadi, H. (2024). Decentralized AI-based task distribution on blockchain for cloud industrial internet of things. *Journal of Grid Computing*, 22(1), article number 33. doi: 10.1007/s10723-024-09751-9.
[26] Kemp, S. (2025). *Digital 2025: Azerbaijan*. Retrieved from https://datareportal.com/reports/digital-2025-azerbaijan.
[27] McKinsey & Company. (2024). *Technology trends outlook 2024*. Retrieved from https://surl.li/irmzke.
[28] Mesquita, L.L., Lizarelli, F.L., Duarte, S., & Oprime, P.C. (2022). Exploring relationships for integrating lean, environmental sustainability and Industry 4.0. *International Journal of Lean Six Sigma*, 13(4), 863-896. doi: 10.1108/IJLSS-09-2020-0145.
[29] Mitra, A., Seetharaman, A., & Maddulety, K. (2024). A structural equation model study for adoption of Internet of Things for the growth of manufacturing industries in Australia. *Journal of Comprehensive Business Administration Research*, 1(2), 93-104. doi: 10.47852/bonviewJCBAR42022482.
[30] Nasser, A.A., Al-Ashwal, M.M., Al-Khulaidi, A.A., Al-Naqeep, A.N., & Al-Jober, M. (2023). A hybrid business-technical model for evaluating iot platforms' functionality, reliability, and usability. *International Journal of Engineering Trends and Technology*, 71(10), 39-59. doi: 10.14445/22315381/IJETT-V71I10P205.
[31] Nozari, H., Fallah, M., & Szmelter-Jarosz, A. (2021). A conceptual framework of green smart IoT-based supply chain management. *International Journal of Research in Industrial Engineering*, 10(1), 22-34. doi: 10.22105/riej.2021.274859.1189.
[32] Organisation for Economic Co-operation and Development. (2022). *Promoting enterprise digitalisation in Azerbaijan*. Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/04/promoting-enterprise-digitalisation-in-azerbaijan_6187d4fa/6a612a2a-en.pdf.
[33] Organisation for Economic Co-operation and Development. (2024). *OECD digital economy outlook 2024 (Volume 2)*. Retrieved from https://www.oecd.org/en/publications/oecd-digital-economy-outlook-2024-volume-2_3adf705b-en.html.
[34] Paiola, M., Schiavone, F., Grandinetti, R., & Chen, J. (2021). Digital servitization and sustainability through networking: Some evidences from IoT-based business models. *Journal of Business Research*, 132, 507-516. doi: 10.1016/j.jbusres.2021.04.047.
[35] Rahimov, E.R., & Rahimov, J.R. (2025). *Nano internet of things*. New York: "Vector" International Publishing House.
[36] Rajabzadeh, M., & Fatorachian, H. (2023). Modelling factors influencing IoT adoption: With a focus on agricultural logistics operations. *Smart Cities*, 6(6), 3266-3296. doi: 10.3390/smartcities6060145.
[37] Salamzadeh, A., Hadizadeh, M., Rastgoo, N., Rahman, M.M., & Radfard, S. (2022). Sustainability-oriented innovation foresight in international new technology based firms. *Sustainability*, 14(20), article number 13501. doi: 10.3390/su142013501.
[38] Saleem, M.U., Shakir, M., Usman, M.R., Bajwa, M.H., Shabbir, N., Shams Ghahfarokhi, P., & Daniel, K. (2023). Integrating smart energy management system with internet of things and cloud computing for efficient demand side management in smart grids. *Energies*, 16(12), article number 4835. doi: 10.3390/en16124835.
[39] Sevak, K.Y., & George, B. (2024). The evolution of Internet of Things (IoT) research in business management: A systematic review of the literature. *Journal of Internet and Digital Economics*, 4(3), 242-265. doi: 10.1108/JIDE-12-2023-0026.
[40] Song, T., Cai, J., Chahine, T., & Li, L. (2021). Towards smart cities by internet of things (IoT) – a silent revolution in China. *Journal of the Knowledge Economy*, 12(2), 1-17. doi: 10.1007/s13132-017-0493-x.
[41] Ullah, A., Anwar, S.M., Li, J., Nadeem, L., Mahmood, T., Rehman, A., & Saba, T. (2024). Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. *Complex & Intelligent Systems*, 10(1), 1607-1637. doi: 10.1007/s40747-023-01175-4.
[42] Valiyev, A., Akhundov, B., Mukhtarova, G., & Ismayilova, N. (2022). *Localizing smart urban development in Azerbaijan*. doi: 10.3929/ethz-b-000525828.

[43] Van Hoang, T. (2024). Impact of integrated artificial intelligence and internet of things technologies on smart city transformation. *Journal of Technical Education Science*, 19(1), 64-73. doi: 10.54644/jte.2024.1532.
[44] Wang, K., Zhao, Y., Gangadhari, R.K., & Li, Z. (2021). Analyzing the adoption challenges of the Internet of things (IoT) and artificial intelligence (AI) for smart cities in China. *Sustainability*, 13(19), article number 10983. doi: 10.3390/su131910983.
[45] World Bank. (2024). *World development report 2024: Data for better lives*. Retrieved from https://www.worldbank.org/en/publication/wdr2024.
[46] World Economic Forum. (2024). *IDEA: Investing in the digital economy of Azerbaijan*. Retrieved from https://www3.weforum.org/docs/WEF_IDEA_Investing_in_the_Digital_Economy_of_Azerbaijan_2024.pdf.
[47] Xing, L. (2024). Evaluation of the impact of artificial intelligence and intelligent Internet of Things on population mobility on regional economic differences. *Soft Computing*, 28, 13977-13988. doi: 10.1007/s00500-023-08351-1.
[48] Yavuz, O., Uner, M.M., Okumus, F., & Karatepe, O.M. (2023). Industry 4.0 technologies, sustainable operations practices and their impacts on sustainable performance. *Journal of Cleaner Production*, 387, article number 135951. doi: 10.1016/j.jclepro.2023.135951.

Сергій Шевченко
Кандидат економічних наук, доцент
Національний університет «Львівська політехніка»
79013, вул. Степана Бандери, 12, м. Львів, Україна
https://orcid.org/0000-0002-5522-3258

Безпека ланцюгів постачання в контексті сталого розвитку: світові практики та український контекст

Анотація. Актуальність дослідження зумовлена зростаючою вразливістю глобальних ланцюгів постачання в умовах збройних конфліктів, геополітичної нестабільності та посилення ризиків для сталого розвитку. Метою дослідження була систематизація підходів до забезпечення безпеки ланцюгів постачання та обґрунтування її ролі як ключового чинника сталого розвитку з урахуванням міжнародного досвіду та українського контексту. Методологічна основа базована на системному аналізі наукової літератури, порівняльному аналізі міжнародних програм безпеки, а також методах синтезу й узагальнення, що дозволило виявити ключові закономірності, фактори ризику та інституційні механізми захисту ланцюгів постачання. Встановлено, що вразливість ланцюгів постачання зумовлюється не лише зовнішніми шоками, такими як військова агресія та руйнування інфраструктури, але й внутрішніми структурними характеристиками сучасних логістичних систем, зокрема розгалуженими мережевими конфігураціями та стратегіями мінімізації запасів. Визначено, що ефективна безпека досягається через інтегровані, ризик-орієнтовані та партнерські моделі, які поєднують державно-приватну взаємодію, попередній обмін інформацією та диференційовані механізми контролю. Аналіз міжнародних програм (C-TPAT, FAST, CSI, AMR) продемонстрував їхню ефективність у підвищенні стійкості ланцюгів постачання при збереженні ефективності торгівлі. Український кейс підтвердив, що масштабні порушення транспортної інфраструктури спричиняють системні економічні, соціальні та екологічні наслідки, безпосередньо впливаючи на сталий розвиток. Обґрунтовано, що безпека ланцюгів постачання виступає наскрізним чинником, який поєднує економічну безперервність, соціальну стабільність та екологічну відповідальність. Практичне значення результатів полягає в можливості їх використання органами державної влади, менеджерами з логістики та підприємствами для розроблення адаптивних, стійких і безпеково орієнтованих моделей управління ланцюгами постачання в умовах кризи та післявоєнного відновлення

Ключові слова: транспортна інфраструктура; логістична стійкість; управління ризиками; державно-приватне партнерство; порушення інфраструктури; міжнародна торгівля; післявоєнне відновлення