Kateryna Molchanova
Candidate of Economic Sciences,
Senior Lecturer at the Department of International Business and Logistics
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»

Молчанова К.
кандидат економічних наук,
старший викладач кафедри міжнародного бізнесу та логістики
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

DOI: https://doi.org/10.30525/978-9934-26-639-3-36

RISKS OF USING DIGITAL TOOLS IN SUPPLY CHAIN MANAGEMENT

РИЗИКИ ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ В УПРАВЛІННІ ЛАНЦЮГАМИ ПОСТАЧАНЬ

It is impossible to imagine today's life without the digital environment. Most people in developed countries spend a significant part of their day in virtual space. These are social networks, entertainment, and of course work processes. Automation and digitalization have very quickly changed almost all areas of production of goods and services. Information technologies are changing not only approaches to organizing and managing business, but also business processes themselves.

The supply chain management sector is the industry that is most actively implementing digital technologies. Blockchain, Internet of Things, Big Data and Analytics, Artificial Intelligence, Robotics are all actively used by supply chain actors. The purpose of using digital tools by logistics companies is to increase operational efficiency, optimize costs, and increase customer satisfaction.

Accordance with researches The Supply Chain Digital Transformation Market size was valued at USD 1207.79 million in 2024 and is expected to reach USD 2931.16 million by 2033, growing at a CAGR of 10.3% from 2025 to 2033 [1]. It is indicated that the global number of companies that implemented at least one type of digital technology in supply chain management in 2024 was 77300. For comparison, in 2022 this number was 52800, that is, the increase in two years was 46,4%.

Digital transformation provided full, real-time transparency across complex, multi-tier supply chains, greatly enhancing operational efficiency and agility. In 2024, 43% of manufacturing companies relied on AI-driven predictive analytics to evaluate supplier performance and anticipate potential disruptions.

More than 17500 organizations adopted IoT sensors to monitor shipments and warehouses in real time, leading to a 22% decrease in inventory shrinkage. The capability to foresee risks and act proactively has become a key priority, especially in the automotive, electronics and retail sectors.

One of the most obstacles to digital transformation in supply chains is the shortage of qualified personnel. In 2023 more than 49% of companies reported that gaps in internal capability caused delays in their digital initiatives. Additionally, the challenge of integrating legacy systems, ERP components and cloud platforms continues to hinder progress. Over 12000 organizations postponed their digital transformation efforts due to integration breakdowns, inconsistent data or compliance-related issues – particularly in highly regulated sectors like pharmaceuticals and aerospace.

The largest players in the supply chain management digital transformation market are IBM and SAP SE. In 2024, IBM led the supply chain digital transformation market with over 3,200 enterprise deployments globally. The company's AI and blockchain-based logistics platforms were integrated by 9 of the top 15 global logistics providers. SAP SE held the second-largest market share, supporting over 2,900 enterprises with end-to-end supply chain management solutions. Their platforms improved planning accuracy by 23% across Europe and Asia-Pacific [1].

When we analyse the pace of digital transformation of the industry, we should not forget that the implementation of digital technologies involves not only obtaining benefits, but also an increase in the associated risks and threats.

Cybersecurity became a significant concern in 2023 and 2024. In 2023 more than 6900 reported cyberattacks targeted supply chain platforms, especially those managing sensitive procurement and vendor information. On average, each incident caused 18 hours of downtime, resulting in millions of dollars in operational losses. At the same time, rising prices for enterprise software licenses, IT infrastructure and cloud storage increased financial strain on SMEs with over 31% reporting that high costs delayed their technological adoption.

Cyber Supply Chain Attacks (CSCAs) are threats that make use of trusted channels (external tiers, goods, and data) in the supply chain in order to compromise the final target, particularly via operational endpoint vulnerabilities. Furthermore, CSCAs in a broader sense are threats that directly impair operations at different points along the supply chain (for example production, distribution, and logistical operations from Original Equipment Provider (OEM) across Module or Supplier System (Tier 1) and Component Supplier (Tier 2) to Parts Supplier (Tier 3) [2]. A report from Cybersecurity Ventures states that the global cost of software supply chain attacks could reach nearly $138 billion, with damage expenses anticipated to increase by 15% annually [3].

According to the Cowbell report, five key technology categories present notable cyber risk: operating systems, content management tools, virtualization platforms, server-side technologies and business applications [4]. Among these

categories, operating systems pose the greatest immediate threat because they form the foundational layer of an organization's entire IT infrastructure.

Supply chain can be big and complicated and keeping them secure is tough because weaknesses can appear or be used anywhere along the way. This makes it hard to know if the whole supply chain is fully protected. Supply chain attacks are hard to spot because they take advantage of trusted connections between organizations and their vendors, software providers or contractors. Despite their complexity there are proven strategies to minimize and reduce potential damage. So, almost any modern technology has its advantages and disadvantages. The main task of companies before implementing a new digital technology is to responsibly assess both the benefits and possible risks and threats.

References:

1. Supply Chain Digital Transformation Market. *Market Reports World*. Available at: https://www.marketreportsworld.com/market-reports/supply-chain-digital-transformation-market-14715179.
2. Kern E., Szanto A. Cyber Supply Chain Attacks. *Brandenburg Institute for Society and Security.* 2022. Available at: https://www.researchgate.net/publication/369750209_Cyber_Supply_Chain_Attacks.
3. 2023 Software Supply Chain Attack Report. *SNYK*. URL: https://surl.li/detexy.
4. Supply chain cyber attacks surge over 400%, expected to continue rising – Cowbell report. *Insurance Business.* Available at: https://www.insurancebusinessmag.com/us/news/cyber/supply-chain-cyber-attacks-surge-over-400-expected-to-continue-rising--cowbell-report-525369.aspx.