СЕКЦІЯ «ЛОГІСТИКА»

Голова: **Смерічевська С. В.**, д.е.н.,проф., в. о. зав. каф. логістики, ФТМЛ

Секретар: **Щеховська Л. М.**, ст. викл.

UDC 004.056.5: 65.012.8

CYBERSECURITY RISKS IN LOGISTICS

Kateryna Barda
National Aviation University, Kyiv

Scientific advisor - Kateryna Molchanova, PhD in Economic, Associate Professor

Keywords: logistics, cybersecurity, risks, technology, protection.

In today's economy, logistics plays an extremely important role in ensuring the efficient movement of goods from the producer to the end consumer. Its importance lies in the responsibility for supply chain management, organization of warehouse logistics, transportation and distribution. However, the growing importance of logistics is accompanied by an increase in cybersecurity threats.

Logistics relies on a huge amount of digital data that is subject to cyber threats. This data includes information about suppliers, orders, and the movement of goods. Protecting information systems in this industry requires a comprehensive approach to cybersecurity, including the use of data encryption, anti-virus software, and staff training.

Understanding cybersecurity risks in logistics plays a key role in ensuring supply chain security and stability. Cyberattacks on industrial enterprises can cause serious disruptions in the supply of components and raw materials, which negatively impacts the productivity and efficiency of production processes. For example, the attack on the automaker Renault-Nissan in 2017 led to the suspension of production at several plants in different countries, which once again emphasizes the importance of protecting industrial systems from cyber threats.

Secondly, cybersecurity risks are of great importance for the FMCG supply chain, which plays a critical role in providing vital goods. For example, a cyberattack on Tesco hypermarket in 2021 led to the temporary paralyzation of its eCommerce system, which caused difficulties in the ordering and delivery of goods to consumers.

Thirdly, the importance of understanding cybersecurity risks is evident in the retail sector, where even the smallest breaches can have significant consequences due to the large number of consumers. For example, an attack on Target's network in 2013 resulted in the leakage of personal data of millions of customers, which led to serious financial losses and damage to the company's reputation [1].

To mitigate cybersecurity risks in logistics, a comprehensive approach must be adopted. It is important to regularly audit and update cyber defenses, identify and eliminate potential vulnerabilities in information systems. In addition, it is necessary to provide cybersecurity training to staff and establish strict policies for access to systems and data [2].

The use of modern technologies can help improve cybersecurity in logistics. For example, the use of blockchain to secure cargo and transaction data can ensure that it is inaccessible to attackers. Artificial intelligence and machine learning technologies can detect anomalies and potential cybersecurity threats by analyzing large amounts of data. In addition, other measures, such as cyber analytics and DDoS protection, can also be used to improve cybersecurity in logistics [3].

The synergy of these aspects - awareness of the impact of cybersecurity breaches, application of risk mitigation strategies, use of modern technologies and their practical implementation - can significantly increase the level of cybersecurity in logistics and make logistics companies more resilient to cyber threats.

Keeping up-to-date with current legal requirements and standards in the field of cybersecurity is extremely important for logistics companies. There are some of the most importrant documents in the cybersecurity: GDPR (General Data Protection Regulation); PSD2 (Revised Payment Services Directive); ISO 27001 is an international standard for an information security management system; PCI DSS (Payment Card Industry Data Security Standard); BSA (Bank Secrecy Act); GLBA (Gramm-Leach-Bliley Act); SOX (Sarbanes-Oxley Act); FINRA is a regulator that controls securities trading and protects customer data. NIST 800-53 is a security standard for federal information systems in the United States. SWIFT CSP is a SWIFT customer security program that includes 22 security measures. CCPA (Consumer Confidentiality Protection Act) [4].

Conclusion.

With the growth of the modern economy, logistics has become key to the efficient movement of goods from producer to consumer. However, this progress has been accompanied by an increase in cybersecurity threats, which can negatively impact the security and stability of supply chains. A comprehensive approach, such as auditing and updating cyber defenses, staff training, and the use of modern technologies, can significantly reduce these risks. The synergy of these measures can improve supply chain security, increase the efficiency of production processes, and strengthen consumer confidence in logistics services in the digital age.

References:

1. Ключові проблеми кібербезпеки в логістиці та їх рішення. *Wezom*. URL: https://wezom.com.ua/ua/blog/klyuchovi-problemi-kiberbezpeki-v-logistitsi-ta-yih-rishennya (access date: 20.03.2024).

2. 7 загроз кібербезпеки у сфері логістики. *Wezom*. URL: https://wezom.com.ua/ua/blog/7-zagroz-kiberbezpeki-u-sferi-logistiki (access date: 20.03.2024).

3. Гузенко С. Як логістичній галузі відповісти на нові виклики кібербезпеки. *Центр транспортних стратегій*. URL: https://cfts.org.ua/blogs/yak_logistichniy_galuzi_vidpovisti_na_novi_vikliki_kiberbezpeki_654 (access date: 20.03.2024).

4. Відповідність вимогам кібербезпеки для фінансової індустрії. *ESKA*. URL: https://eska.global/blog/vidpovidnist-vimogam-kiberbezpeki-dlya-finansovoyi-industriyi (access date: 20.03.2024).