UDC 004.056.2

Valentyn Yanchuk, PhD, professor,
Anna Humeniuk, PhD, professor
Zhytomyr Polytechnic State University

DATA AND APPLICATION SECURITY ASPECTS FOR INTERNATIONAL E-COMMERCE SOLUTIONS IN EUROPE AND UKRAINE FROM THE PERSPECTIVE OF DATA PROTECTION AND SUPPLY CHAIN MAINTENANCE

Accelerated integration of the Ukrainian digital economy into the European Single Market has created unprecedented opportunities for cross-border e-commerce. However, scaling operations across these jurisdictions introduces complex challenges at the intersection of data protection compliance, advanced application architecture security, and physical and digital supply chain integrity. Unlike domestic operations, international e-commerce solutions must navigate a bifurcated regulatory landscape while maintaining seamless operational continuity against an evolving threat landscape. This thesis examines the technical and organizational imperatives for securing these cross-border platforms, extending beyond basic transactional security to include complex product configuration systems and international logistics data flows.

The research on this subject is performed in the frame of fellowship under the Polish National Commission for UNESCO 2025/2026 Ref. 205/E/2025 JM.4020.54.2025

The foundation of international e-commerce security in this context lies in harmonizing regulatory requirements. While Ukraine is actively aligning its legislation with European standards, significant operational gaps remain between domestic laws and the General Data Protection Regulation (GDPR). For e-commerce entities operating between Ukraine and the EU, the primary challenge is ensuring lawful cross-border data transfer mechanisms. The architecture must support strict data localization requirements where necessary, while facilitating the flow of transactional data essential for commerce. This requires implementing robust "Privacy by Design" principles directly into the application architecture, ensuring that data subject rights can be executed technically across distributed databases located in different jurisdictions [1].

From an application security perspective, the reliance on monolithic architectures is rapidly becoming a liability in international trade. Modern cross-border e-commerce relies heavily on microservices and extensive API integrations connecting storefronts in one country with logistics providers, payment gateways, and warehousing services in others. Consequently, API

security has emerged as the critical attack surface. Traditional perimeter defenses are insufficient when data constantly flows between Ukrainian specialized services and EU fulfilment centers. Security measures must shift towards rigorous API gateway controls, implementing mutual TLS (mTLS) for service-to-service authentication across borders, and adhering strictly to standards such as the OWASP API Security to prevent broken object level authorization and excessive data exposure in transit [2].

A significant development in modern e-commerce is the rise of complex product configurators, allowing customers to customize goods prior to ordering. These sophisticated frontend tools introduce unique security vectors often overlooked in traditional threat models. Complex configurators frequently rely heavily on client-side logic for interactivity, making them vulnerable to business logic manipulation, such as price tampering or inventory bypass attacks, if client-side validation is trusted blindly. Furthermore, the configuration data itself –representing manufacturing specifications –constitutes sensitive intellectual property. Securing these systems requires rigorous server-side re-validation of complex configuration data structures and ensuring state integrity throughout the customization process to prevent the injection of malicious parameters into the manufacturing workflow [3].

Furthermore, the concept of supply chain maintenance in international e-commerce has expanded to include both the digital software supply chain and the physical logistics data chain. E-commerce platforms depend on a complex ecosystem of third-party libraries and SaaS integrations. A vulnerability in a third-party module used by a Ukrainian vendor can compromise data integrity for European customers, necessitating rigorous Vendor Risk Management (VRM) programs [4].

Simultaneously, the physical aspect of supply chain maintenance – logistics between Ukraine and the EU –presents critical data protection challenges regarding problem-solving in transit. The integration of Ukrainian carriers with pan-European logistics networks requires real-time data exchange regarding customs declarations, routing optimization, and IoT-based tracking. The integrity of this data is paramount; manipulation of shipping manifests or customs data in transit can lead to severe operational disruptions, regulatory penalties at the border, and fraud. Securing these logistics data flows requires immutable audit trails for custody transfer and ensuring that IoT devices used for tracking shipments across borders are secured against compromise to prevent them from becoming entry points into the wider logistics network [5].

In conclusion, securing international e-commerce solutions between Europe and Ukraine requires a holistic strategy that transcends basic compliance. It demands an architectural shift towards Zero Trust principles

for cross-border API interactions, deep visibility into both software and logistics data supply chains, and robust validation mechanisms for complex frontend configurators. Only by integrating these advanced data protection measures directly into the technical fabric of the platform can organizations maintain the trust and operational integrity necessary for sustained international growth.

References:

1. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. DOI: https://doi.org/10.1093/cybsec/tyw001. Last access: 24/11/2025

2. Alshaikh, M. (2020). Developing cybersecurity culture to influence cybersecurity policy compliance: A conceptual framework. Computers & Security, 98, 102003. DOI: https://doi.org/10.1016/j.cose.2020.102003. Last access: 24/11/2025.

3. Quintus, M., Mayr, K., Hofer, K. M., & Chiu, Y.-T. (2024). Managing consumer trust in e-commerce: Evidence from advanced versus emerging markets. International Journal of Retail & Distribution Management, 52(10-11), 1038-1056. DOI: 10.1108/IJRDM-10-2023-0609. Last access: 24/11/2025.

4. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontiers in Psychology, 13, Article 927398. DOI: 10.3389/fpsyg.2022.927398. Last access: 24/11/2025.

5. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134–153. DOI: https://doi.org/10.1016/j.clsr.2017.05.015. Last access: 24/11/2025.