

# INTEGRATION OF DIGITAL PAYMENT SYSTEMS IN E-COMMERCE AS A KEY FACTOR OF ENTERPRISE ECONOMIC SECURITY

## ІНТЕГРАЦІЯ ЦИФРОВИХ ПЛАТІЖНИХ СИСТЕМ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ ЯК КЛЮЧОВИЙ ФАКТОР ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

*The article explores the integration of digital payment systems into e-commerce as a key factor in strengthening enterprise economic security. It emphasises the strategic role that digital payments play in ensuring financial stability, reducing operational risks, and enhancing customer trust, especially for small and medium-sized enterprises (SMEs). The study synthesises current academic discourse and industry reports, focusing on the advantages of real-time transaction processing, transparency, compliance with regulatory standards, and operational efficiency. It highlights the risks associated with cybersecurity threats, platform interoperability, and legal non-compliance. Empirical insights are drawn from the integration experiences of Eastern European SMEs using platforms such as PayPal, LiqPay, and Fondy. In addition, the article examines the transformative potential of blockchain-based systems, artificial intelligence, and decentralized finance technologies in reshaping payment infrastructures. It concludes that the integration of secure and innovative digital payment systems is not merely a technological upgrade, but a strategic necessity that directly supports economic resilience and long-term competitiveness in the digital economy.*

**Key words:** digital payments, e-commerce, economic security, fintech, blockchain, entrepreneurship, payment platforms.

У статті висвітлено теоретико-прикладні аспекти інтеграції цифрових платіжних систем у сферу електронної комерції як одного з базових інструментів забезпечення економічної безпеки підприємств в умовах цифровізації та динамічного розвитку фінансово-технологічного середовища. Обґрунтовано, що цифрові платіжні системи відіграють ключову роль не лише у спрощенні фінансових розрахунків, а й у створенні основи для прозорості, стійкості та конкурентоспроможності бізнесу в цифровій економіці. Особливе значення ця інтеграція має для малих і середніх підприємств, які потребують ефективних рішень для оптимізації грошових потоків, зниження транзакційних витрат і посилення довіри з боку споживачів. У роботі визначено, що цифрові платіжні системи – такі як PayPal, Fondy, LiqPay, Stripe, Apple Pay і Google Pay – забезпечують високий рівень автоматизації, інтеграції з ERP/CRM-системами, підтримку багатовалютних розрахунків та відповідність міжнародним стандартам безпеки, зокрема PCI DSS, KYC та AML. Акцентовано на необхідності дотримання підприємствами регуляторних вимог як на міжнародному (зокрема, GDPR у межах ЄС), так і національному рівнях. У результаті системного аналізу функціональних характеристик вказаних платформ з'ясовано, що якісна інтеграція платіжної інфраструктури безпосередньо впливає на ефективність бізнес-процесів, фінансову дисципліну та можливості прогнозування на основі обробки великих обсягів транзакційних даних. Окрема увага приділена ризикам, що супроводжують процес цифрової інтеграції: кіберзагрози, витоки даних, шахрайство, проблеми сумісності та недостатній рівень цифрової компетентності персоналу. Водночас сучасні технології, такі як штучний інтелект, машинне навчання, блокчейн і DeFi-платформи, мають потенціал трансформувати систему цифрових платежів у бік більшої автономності, прозорості та економічної вигоди. За даними дослідження, проведеного в Україні серед представників малого бізнесу, повноцінна інтеграція платіжних шлюзів сприяє зростанню задоволеності клієнтів, збільшенню повторних покупок і зменшенню кількості помилок при обробці платежів. Зроблено висновок, що інтеграція цифрових платіжних систем має розглядатися не лише як технічний процес, а як елемент стратегічного управління, що охоплює фінансову, операційну та репутаційну компоненти економічної безпеки. Запропоновані рекомендації спрямовані на підвищення адаптивності підприємств до цифрових викликів, формування довгострокової платоспроможності та покращення взаємодії з цифровими споживачами.

**Ключові слова:** цифрові платежі, електронна комерція, економічна безпека, фінансові технології, блокчейн, підприємництво, платіжні платформи.

UDC: 004.738.5:336.71

DOI: <https://doi.org/10.32782/dees.17-33>

**Necheporenko Illia<sup>1</sup>**

Postgraduate Student  
at the Department of Economic  
Cybernetics,  
Sumy State University

**Hrytsenko Kostiantyn<sup>2</sup>**

PhD in Technical Sciences,  
Associate Professor,  
Associate Professor at the Department  
of Economic Cybernetics,  
Sumy State University

**Нечепоренко І.Д.**

Сумський державний університет

**Гриценко К.Г.**

Сумський державний університет

**Formulation of the problem.** In the context of rapid global digitalisation and the expansion of the e-commerce sector, digital payment systems have emerged as essential infrastructure for online transactions. Their proper integration not only facilitates business operations but also strengthens the financial stability and strategic resilience of enterprises. For small and medium-sized enterprises (SMEs), in particular, secure digital payments are

critical for minimizing transactional risks, optimizing cash flow, and enhancing customer experience [1]. However, the increasing complexity of digital finance creates new challenges in cybersecurity, regulatory compliance, and interoperability between platforms. Addressing these challenges is a priority for ensuring economic security in the digital age.

**Analysis of recent research and publications.** Recent academic and industry studies emphasise the

<sup>1</sup> ORCID: <https://orcid.org/0009-0007-4748-1592>

<sup>2</sup> ORCID: <https://orcid.org/0000-0002-7855-691X>

growing importance of digital payments as both a technological and strategic asset. Yakubiv et al. [2] noted the transformative impact of payment digitalisation on Ukraine's financial system, pointing to increased transaction speed, accessibility, and automation. At the same time, reports by global organizations such as the World Bank [3] and OECD [4] draw attention to risks related to data security, fraud, and regulatory gaps.

Yatsukh et al. [5] explored the role of digital innovation in the banking sector and emphasised the need for robust integration between payment systems and internal enterprise processes. According to a report by McKinsey [6], 89% of consumers expect seamless, instant digital transactions, which forces enterprises to rethink their payment infrastructure. While many solutions exist (e.g., Stripe, PayPal, Apple Pay, Google Pay), the challenge lies in choosing systems that align with the business model, market regulations, and consumer expectations.

Despite the progress in this area, unresolved issues remain, particularly concerning risk management, the economic efficiency of payment innovations, and strategic integration into enterprise systems. This article addresses these gaps by exploring how payment system integration affects enterprise economic security.

**Formulating the purpose of the article.** The purpose of this article is to analyse the role of digital payment system integration in e-commerce enterprises and to evaluate its influence on enterprise economic security, considering technological, financial, and operational dimensions.

**Presentation of the main research material.** In recent years, the spreading of digital payment systems has profoundly transformed the structure and dynamics of e-commerce. As enterprises strive to optimize their financial operations and respond to rapidly evolving consumer expectations, the integration of digital payment platforms has emerged as a strategic imperative. This process, however, is not solely technological in nature – it is deeply intertwined with the economic security of enterprises, as it affects the stability, transparency, and efficiency of financial flows.

Digital payment systems offer a wide range of functionalities, from basic online transactions to advanced integration with accounting, customer relationship management, and enterprise resource planning systems. Their ability to process payments in real-time, across borders, and in multiple currencies reduces delays and facilitates uninterrupted business operations. Such efficiency is especially vital in e-commerce, where consumer decisions are often influenced by the ease and reliability of the checkout process. Enterprises that provide frictionless and secure payment options are more likely to achieve higher conversion rates and customer retention [7].

From the standpoint of economic security, integrated digital payment systems play a protective

role by minimizing financial and operational risks. Automated transaction logging, for instance, enhances internal control mechanisms, enabling faster and more accurate financial audits. This reduces opportunities for internal fraud, accounting manipulation, and human error. Moreover, by incorporating encryption technologies, tokenization, biometric authentication, and two-factor verification, modern payment platforms ensure a high level of transaction security. These security mechanisms foster consumer trust – an essential asset in the hypercompetitive e-commerce environment [8].

Nonetheless, the integration of such systems is not without its challenges. Cybersecurity remains a persistent threat, as digital payment platforms are frequent targets for data breaches, phishing attacks, and ransomware. According to the European Central Bank, the number of reported cyber incidents involving payment systems grew by over 20% in 2023, with small and medium enterprises being particularly vulnerable due to limited IT infrastructure and expertise [9]. Consequently, a robust integration strategy must include risk assessment, staff training, constant monitoring, and collaboration with cybersecurity vendors.

An illustrative case can be seen in the Ukrainian SME sector, where the adoption of hybrid payment ecosystems – comprising both global services like PayPal and local platforms such as Fondy and LiqPay – led to a significant decrease in payment rejection rates and operational delays. A 2023 survey conducted by the Ministry of Digital Transformation of Ukraine revealed that enterprises that fully integrated digital payment gateways into their operations reported a 36% improvement in customer satisfaction and a 22% rise in repeat purchases within twelve months [10].

For a comparative understanding of key digital payment platforms used in Eastern European e-commerce environments, Table 1 summarizes critical attributes including transaction speed, fees, integration capabilities, multi-currency support, and regulatory compliance.

Equally important is the regulatory landscape. Payment system integration must comply with a series of international standards and national regulations, including the Payment Card Industry Data Security Standard, anti-money laundering directives, know-your-customer protocols, and, in the case of the European Union, the General Data Protection Regulation. Failure to adhere to these frameworks can result in severe financial penalties and reputational damage. Therefore, enterprises must select systems that not only meet functional requirements but also ensure legal and regulatory compliance [11].

Moreover, the integration of digital payment systems contributes to strategic financial planning and forecasting. Through access to detailed and real-time transaction data, enterprises can analyse cash

Table 1

Key characteristics of digital payment platforms for business

Payment Platform	Transaction Speed	Average Fee	ERP/CRM Integration	Currency Support	PCI DSS / KYC / AML Compliance
PayPal	Up to 1 minute	2.9% + \$0.30	Medium	25+	Yes
LiqPay	Instant	~1.5%	High	10+	Yes
Fondy	Instant	From 1.3%	High	150+	Yes
Stripe	Up to 1 minute	2.5%	High	135+	Yes
Google Pay	Instant	Built-in	Limited	1–2	Partial
Apple Pay	Instant	Built-in	Limited	1–2	Partial

Source: [8–10]

flow trends, identify seasonal patterns, and optimize inventory and supply chain strategies accordingly. Advanced systems that leverage artificial intelligence and big data analytics further enhance decision-making by providing predictive insights into customer payment behavior, fraud detection, and market trends [12]. For instance, AI-driven solutions embedded within modern payment gateways can detect anomalies in transaction volumes and patterns, flagging suspicious activities before they result in material losses.

The emergence of decentralised finance platforms and blockchain-based payment solutions also introduces new opportunities for enhancing economic security. These technologies offer lower transaction fees, higher transparency, and greater autonomy from traditional financial institutions. While still in the early stages of adoption, especially among smaller enterprises, they hold the potential to revolutionise payment infrastructure by reducing dependency on intermediaries and enabling peer-to-peer financial interactions underpinned by smart contracts [13].

In conclusion, the integration of digital payment systems serves as a critical node in the wider network of digital transformation in e-commerce. It is not simply a means of facilitating financial transactions, but a comprehensive mechanism for ensuring financial resilience, operational integrity, and long-term economic security. Enterprises that treat payment integration as a strategic, data-driven, and secure component of their business model are better positioned to thrive in the digital economy. Such integration must be approached not merely as a technical upgrade, but as a fundamental reconfiguration of the enterprise's financial architecture and customer experience strategy.

**Conclusions.** The conducted research confirms that the integration of digital payment systems is not merely a technical solution but a strategic component of enterprise economic security in the digital age. Through the implementation of modern payment technologies, enterprises – particularly small and medium-sized – gain access to tools that enhance the transparency of financial flows, reduce transactional and operational risks, and build consumer trust by ensuring secure and seamless payment experiences.

The study reveals that successful integration of digital payment platforms leads to improvements in internal control systems, facilitates real-time transaction monitoring, and supports compliance with international security and regulatory standards (such as PCI DSS, KYC, AML, and GDPR). This is particularly important in e-commerce environments where speed, accuracy, and data protection are crucial for maintaining competitive advantage and customer loyalty.

At the same time, the research highlights several systemic challenges. Among them are growing cyber threats, risks of data breaches, the complexity of interoperability with legacy accounting systems, and the need for personnel with appropriate digital competencies. Furthermore, enterprises must navigate an increasingly fragmented regulatory landscape, balancing innovation with compliance.

In this context, strategic planning and proactive risk management emerge as essential prerequisites for the effective deployment of payment solutions. The integration process should include cybersecurity protocols, employee training, and the use of predictive analytics for fraud detection and financial forecasting. Importantly, enterprises that embrace emerging technologies—such as AI, blockchain, and decentralized finance—demonstrate greater resilience and adaptability in turbulent digital environments.

The practical contribution of this study lies in the formulation of recommendations for business leaders on how to select and implement payment platforms based on operational scale, market conditions, and long-term development goals. The findings may serve as a foundation for further empirical research into the correlation between payment system integration and key performance indicators such as customer retention, revenue growth, and transaction efficiency.

Prospects for further research include a deeper examination of regional differences in adoption rates, case studies of integration models across sectors (e.g., retail vs. services), and the long-term effects of decentralized finance on enterprise-level financial governance. Additionally, quantitative analysis of the return on investment (ROI) from payment technology implementation would provide valuable insights for decision-makers.

# REFERENCES:

1. Schneider S., Sunyaev A. (2016). Determinant factors of cloud-sourcing decisions: Reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology*, vol. 31(1), pp. 1–31. DOI: <https://doi.org/10.1057/jit.2014.25>
2. Yakubiv V., Sodoma R., Shmatkovska T., Dziamulych M., Brodskal. (2020). Digitalization of payment systems in Ukraine. *International Journal of Recent Technology and Engineering*, vol. 8(5), pp. 4590–4596.
3. World Bank. (2018). Digital Financial Services: Challenges and Opportunities for Emerging Market Banks. Available at: <https://openknowledge.worldbank.org/handle/10986/30368>
4. OECD. (2024). Digital Economy Outlook 2024. OECD Publishing. Available at: [https://www.oecd.org/en/publications/oecd-digital-economy-outlook\\_f0b5c251-en.html](https://www.oecd.org/en/publications/oecd-digital-economy-outlook_f0b5c251-en.html)
5. Yatsukh O., Demchenko I., Ilnytsky D., Tsap V., Shmatkovska T. (2021). Management of banking innovations in the conditions of digitalization. *AD ALTA: Journal of Interdisciplinary Research*, vol. 11 (Special issue XVII), pp. 123–127.
6. McKinsey & Company. (2023). The 2023 McKinsey Global Payments Report. Available at: <https://www.mckinsey.com/industries/financial-services/our-insights/the-2023-mckinsey-global-payments-report>
7. Karlin M. I., Shmatkovska T. O., Borysiuk O. V. (2021). Banking innovations in the digital economy formation. *Economy and Society*, no. 27.
8. Accenture. (2023). Digital Payments and Fraud Prevention: A Global Perspective. Available at: <https://bankingblog.accenture.com/one-big-idea-payments-fraud-risk-opportunity>
9. Visa. (2024). Consumer Trust in Digital Payments: Global Insights Report. Available at: <https://km.visamiddleeast.com/content/dam/VCOM/regional/cemea/genericmena/pay-with-visa/security-and-assistance/stay-secure-2024/stay-secure-report.pdf>
10. SAP. (2022). Integration of Digital Payment Systems with ERP: White Paper. Available at: <https://help.sap.com/docs/DIGITALPAYMENTS>
11. European Central Bank. (2023). Cybersecurity in the Financial Sector – Annual Review. Available at: <https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230308~92211cd1f5.en.html>
12. OECD. (2024). Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. Available at: [https://www.oecd.org/en/publications/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine\\_4b13b0bb-en.html](https://www.oecd.org/en/publications/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_4b13b0bb-en.html)
13. PCI Security Standards Council. (2023). Data Security Standard v4.0. Available at: <https://www.pcisecuritystandards.org>