

Introduction of information technologies in international trade in the development of foreign economic activity: Security aspect

Andrij Zaverbnyj*

Doctor of Economic Sciences, Professor
Lviv Polytechnic National University
79013, 12 Stepan Bandera Str., Lviv, Ukraine
<https://orcid.org/0000-0001-7307-536X>

Abstract. The purpose of the article was to study and develop the information support for managing international trade by Ukrainian enterprises under the conditions of expanding the foreign economic activity, considering the security aspect. The theoretical and methodological foundations of the research were based on the application of a comprehensive interdisciplinary approach that effectively combined the economic theory of international trade, information and economic security, risk management, and digital transformation. The main research methods included system analysis, comparative study, and digitalisation analysis. A review of the literature and legal framework on the implementation of innovative information technologies in the international trade of Ukrainian enterprises and the security aspects was conducted. The study emphasised that the security aspect of digitalising the information support of international trade by Ukrainian enterprises is of considerable importance. Security challenges and threats were identified as key barriers to the digital transformation of foreign economic activity, particularly international trade. The peculiarities of using information technologies in foreign economic activity are revealed, especially in the context of digital transformation, cybersecurity, and regulatory compliance. The prospects opened by integrating digital solutions such as electronic platforms, blockchain, big data, and artificial intelligence are outlined. Proposals have been developed to enhance the level of information security under the conditions of globalisation and digitalisation of world trade relations. A sequence of information support for managing international trade by Ukrainian enterprises in the process of developing the foreign economic activity, considering the security aspect, has been proposed. Information systems capable of assessing the competitive environment, taking into account all macroeconomic, institutional, microeconomic, security, and other market factors relevant to enterprises – measuring, assessing, and forecasting competition within industries, countries, and regions, as well as identifying technological lag and customer needs (especially new ones when entering foreign markets) – have been identified. It has been established that, to ensure the effective operation of an enterprise, particularly in the context of foreign economic activity, it is necessary to create a reliable information system capable of meeting the complex needs of the enterprise over a long period of time

Keywords: digitalisation; globalisation; economic security; information; cybersecurity

Introduction

The issue of developing, implementing and actively using information technologies (IT) by enterprises in the international trade has become extremely relevant in view of the reforms and digitalisation of country's economy, the dynamism, and globalisation of the world economy. After all, trends in the global economy make digitalisation a key factor in increasing the efficiency of international trade.

Ukrainian enterprises, actively expanding the participation in foreign economic activity, are increasingly facing the urgent need to introduce the latest IT to ensure the required level of the own competitiveness, transparency, and security of trade (including international) operations. Along with the potential of digital solutions, there are also serious challenges and threats associated with cyber threats (especially

Suggested Citation:

Zaverbnyj, A. (2025). Introduction of information technologies in international trade in the development of foreign economic activity: Security aspect. *Innovation and Sustainability*, 5(3), 66-78. doi: 10.31649/vis/3.2025.66.

*Corresponding author



in 2014-2025), imperfect infrastructure, and low levels of digital culture in certain business segments.

I.Z. Savras & V.I. Fedynets (2023) examined the role of digitalisation in the innovative development of enterprises, in particular the positive effects of digitalisation on innovation, obstacles to the implementation of innovations in the context of digitalisation. H. Blakyta *et al.* (2025) noted that the issue of digitalisation and its impact on various spheres of society and on the activities of enterprises and organisations has been one of the most pressing in many areas of scientific research. Digital technologies were defined as a driver of sustainability and adaptability for Ukrainian enterprises, which underscored the importance of researching this topic. H. Blakyta *et al.* (2025) also noted that it was precisely the crisis conditions (the COVID-19 epidemic, war) that prompted Ukrainian enterprises to intensify the use of digital technologies. However, researchers have focused on conceptual theoretical and methodological issues, while quantitative studies of digitalisation and digital transformation have not gained sufficient traction, primarily due to a lack of data.

Digital transformation in organisational management is a complex, multifaceted process that requires an integrated approach combining technical and organisational aspects. A. Drabovskiy (2025) pointed to the successful implementation of a digital strategy as a significant result. It depends on the formation of a digital culture within the enterprise and the improvement of the digital competencies of the management team. As the author pointed out, transformational leadership plays a significant role in this process, as it is capable not only of adapting the organisation to new conditions, but also of initiating innovation and promoting the active participation of all levels of staff in the implementation of changes.

The issue of currency security was examined by B. Il-ychok *et al.* (2024). The authors devoted the research to improving the effectiveness of public administration in the field of currency security in Ukraine. The researchers provided a general description of the essence, state, and dynamics of the effectiveness of public administration of the state's currency security. The authors also assessed the state and dynamics of Ukraine's currency security indicators based on the characteristics of the state's currency policy indicators compared to similar indicators in Poland. A Danish company named Maersk (2022) in the research on the digitisation of the supply chain and increasing innovation in the industry, used solutions aimed at reducing trade disputes and promoting the development of global trade. It should also be noted that the issue of digitalisation is relevant in various spheres of life in Ukraine. O. Bulavynets (2025) studied the essence of digitalisation of social transfers as an important step for further modernisation of social protection systems and increasing the efficiency of the administration. According to the study, digitalisation involves the integration of modern IT to automate the processes of providing social benefits, ensuring accessibility, transparency, and speed in the distribution of social

assistance, including that received from abroad. It was important to note O. Bulavynets (2025) conclusion that the processes of introducing digital technologies pose new challenges for the state: the need to ensure cybersecurity, protect personal data, and train the population to use new tools.

In dynamic conditions of globalisation and digital transformation of the economy, information technology plays and will continue to play a key role in the development of such international economic relations as international trade. Enterprises, actively developing the foreign economic activity, implement modern IT solutions that serve as a tool for improving the efficiency of foreign economic operations, a prerequisite for maintaining the competitiveness of these enterprises and the products and services in the global market. The process of integrating modern information and communication technologies into foreign economic activity is usually accompanied by several problems: insufficient, outdated, inflexible digital infrastructure in the country or region, limited opportunities for financing the implementation and use of these technologies, staff shortages (especially in times of war), legislative and regulatory barriers, etc. These problems create challenges for enterprises in the digitalisation of the international trade operations, logistics, customs clearance, e-commerce, use of analytical platforms. Despite significant achievements in the field of introduction of modern IT into international trade of Ukrainian enterprises in the context of the foreign economic activity, the security aspect of these processes has not been sufficiently systematised and studied. The aim of the study was to analyse the issues surrounding the implementation of up-to-date IT in the international trade of Ukrainian enterprises, taking into account security aspects.

Materials and Methods

The study used a comprehensive interdisciplinary approach that integrated the provisions of the economic theory of international trade, information security theory, economic security, risk management, and the concept of digital business transformation. This approach was used to comprehensively examine the issues of digitalisation of information support for foreign economic activity of enterprises under martial law. The study was based on the following methods. The system analysis allowed covering the interrelationships between information security, digital solutions, and the peculiarities of the functioning of enterprises in the context of foreign economic activity. The method of comparative research was used to analyse the current regulatory framework in the field of information security and digitalisation in Ukraine in comparison with international standards and practices. The review and analytical methods were applied to study literary sources (Tron, 2016; Lupak, 2019; Glushchewsky *et al.*, 2023) and statistical materials on the level of digitalisation, IT infrastructure, and cyber threats in the field of international trade. Analysing digital solutions (technologies), including the use of electronic data interchange (EDI), enterprise resource planning (ERP), customer relationship management (CRM), blockchain, big data,

and cloud services, allowed determining the level of readiness of Ukrainian enterprises for digital transformation in international trade. The following companies were selected for analysis: Nova Poshta (n.d.), PrivatBank (n.d.), SoftServe (2024), with one state structure (The State Cyber Protection Centre..., 2024). The companies were selected because these companies were recognised leaders in Ukraine both in terms of gross income and in the implementation of information technologies in international trade within the development of foreign economic activity.

The methodology of the study also included a number of Ukrainian laws: Law of Ukraine No. 675-VIII (2015), Law of Ukraine No. 1789-VIII (1992), Law of Ukraine No. 2155-VIII (2017), Law of Ukraine No. 2297-VI (2010), Law of Ukraine No. 851-IV (2003), as amended in 2023, Law of Ukraine No. 1089-IX (2020), as amended in 2025, etc. The selection of these specific Ukrainian laws as a methodological basis was due to their fundamental role in regulating digital processes, ensuring information security, and supporting the digital transformation of international business operations. Law of Ukraine No. 675-VIII (2015) established the legal framework for conducting business activities online, which was directly relevant to international trade, as it provided mechanisms for the validity of electronic contracts and transactions. Law of Ukraine No. 1789-VIII (1992) defined the general principles of information relations, including access, dissemination, and protection of information, which formed the basis for secure data exchange in foreign economic activity. Law of Ukraine No. 2155-VIII (2017) introduced the use of digital signatures, authentication, and trust services that guaranteed the reliability and legal recognition of electronic interactions in cross-border trade. Law of Ukraine No. 2297-VI (2010) ensured compliance with international standards of data privacy and protection, which was crucial when Ukrainian companies engaged in trade with EU and other international partners. The Law of Ukraine No. 851-IV (2003, amended in 2023) regulated the creation, storage, and legal force of electronic documents, thus facilitating secure digital document exchange in foreign trade. Law of Ukraine No. 1089-IX (2020, amended in 2025) provided the legal framework for electronic communication networks and services, which was essential for maintaining cybersecurity and uninterrupted digital interaction in international trade. These legislative acts formed a comprehensive methodological framework for analysing the security dimension of IT implementation in international trade.

The application of international standards such as ISO/IEC 27001:2022 (2022) and the NIST Cybersecurity Framework (n.d.) as methodological foundations for the security aspect of the implementation of information technologies in international trade in the development of foreign economic activity was justified by their global recognition and practical significance in ensuring cybersecurity and information protection. ISO/IEC 27001:2022 (2022) established the international standard for information security management systems (ISMS). Its implementation ensured systematic

risk management, continuous monitoring, and compliance with global requirements for data confidentiality, integrity, and availability. For enterprises engaged in international trade, adherence to ISO/IEC 27001:2022 (2022) strengthened trust with foreign partners and provided evidence of compliance with international security benchmarks. The NIST Cybersecurity Framework (developed by the U.S. National Institute of Standards and Technology) provided a flexible structure for managing cyber risks based on five key functions: identify, protect, detect, respond, and recover. Its use helped businesses establish comprehensive security processes, mitigate cyber threats, and ensure the resilience of cross-border digital operations. By incorporating ISO/IEC 27001:2022 (2022) and the NIST Cybersecurity Framework (n.d.) into the methodological foundation, the study ensured alignment with the best international practices. This not only complemented Ukrainian legislation but also reflected the requirements of global trade partners and international organisations, thereby enhancing the security and competitiveness of Ukrainian enterprises in the global digital economy.

Results

In the context of globalisation and growing cyber threats, the implementation of information technologies in international trade becomes a key factor in the effective development of enterprises' foreign economic activity. Ensuring digital and information security, in turn, is a prerequisite for maintaining the competitiveness and resilience of Ukrainian business in global markets. According to T. Vasylytsiv *et al.* (2017), R. Lupak (2019) and A. Zaverbnyi *et al.* (2024), the key challenges can be grouped into several interrelated areas. First, there is the instability of the IT infrastructure, which reflects the insufficient digital maturity of enterprises and the personnel; this issue will be addressed in more detail later, but it is also compounded by the absence of effective strategies for cyber defence development. A second pressing concern is the imperfection of the existing regulatory framework: the current legislation on protecting commercial and personal information requires substantial harmonisation with international standards and norms. Equally important is the acute shortage of qualified personnel, as the lack of highly skilled IT specialists able to integrate new solutions into enterprises' foreign economic processes hampers international trade; under martial law, this deficit is exacerbated by the mobilisation of mainly men, ongoing rocket attacks, civilian casualties, and intensified emigration flows. Finally, the situation is aggravated by a significant rise in cybersecurity threats, with a growing number of incidents aimed at disrupting supply chains, stealing data, and substituting communications. It is a comprehensive, multi-level system of legislative and regulatory acts aimed at protecting the information space and ensuring the information sovereignty of the state. In the process of developing information technologies in the management of international trade, priority should be given to the general legal principles governing information and

informatisation, integrating these principles into international law. This will allow forming the basis for further integration of specific technological solutions.

The legal framework that establishes the key principles of access to information, its use, and protection comprises the national laws: the Law of Ukraine No. 675-VIII (2015), the Law of Ukraine No. 1789-VIII (1992), the Law of Ukraine No. 2155-VIII (2017), the Law of Ukraine No. 2297-VI (2010), the Law of Ukraine No. 851-IV (2003, amended in 2023), the Law of Ukraine No. 1089-IX (2020, amended in 2025), among others. Collectively, these legal acts form the foundation for the utilisation of information technologies across various domains, including international trade and foreign economic activity. It should be emphasised that this legislative framework is subject to ongoing amendments and additions, reflecting the need to adapt to the international environment and the high dynamism of digitalisation processes. Some amendments are scheduled to be introduced during 2025. The Law of Ukraine No. 675-VIII (2015) defines the organisational and legal principles of e-commerce, including the procedure for concluding electronic transactions, the legal equivalence of electronic and written contracts, consumer rights, and transparency regarding information about sellers and delivery. Its international component lies in the requirement to comply with European data protection standards when dealing with clients from the EU, which has significant implications for companies engaged in cross-border trade. The 2022 edition introduced new provisions, particularly concerning the status of intermediary service providers, such as operators, payment systems, and domain registrars. Nevertheless, problematic aspects remain: the law lacks comprehensive alignment with international practice and UNCITRAL jurisdiction, which creates a regulatory lag. Moreover, the boundary between the extensive liability of sellers and the limited liability of intermediary service providers is not always clearly delineated.

The Law of Ukraine No. 1789-VIII (1992) regulates the fundamental principles of access to information, including the right to obtain, disseminate, and protect it. Although the law does not contain explicit provisions on international trade, it allows for the application of principles aligned with international information standards. Over the years, the law has undergone continuous updates: for instance, between 2010 and 2020, amendments introduced new formats of digital interaction and refined terminology. However, the law continues to face certain challenges: its regulation remains highly fragmented, and it lacks modern provisions on digitalisation, particularly in relation to e-commerce, big data, and related domains.

The Law of Ukraine No. 1089-IX (2020, amended in 2025) comprehensively regulates the field of electronic communications, including the radio frequency spectrum, the competences of public authorities, the rights, and responsibilities of market participants, and user protection. The international dimension of this law is manifested in the implementation of EU standards (notably the European

Electronic Communications Code) as part of Ukraine's Association Agreement with the EU. This ensures Ukraine's gradual convergence with the EU's Digital Single Market. The 2025 edition reinforced this alignment by introducing provisions on general authorisation, out-of-court dispute resolution, and equal conditions for operators. Nevertheless, several challenges remain, including Ukraine's dependence on the European regulatory framework, which may complicate the process of transposition, as well as potential conflicts between infrastructure regulation and the regulation of e-commerce.

Looking forward, it is advisable to focus on the prospects of intensifying the use of digital technologies in the foreign economic activities of enterprises and organisations. Despite existing problems, risks, and threats, digitalisation possesses considerable transformational potential. In particular, the application of blockchain technologies can ensure transparency and integrity of international contracts, traceability of goods, and the prevention of document falsification – factors of critical importance in turbulent and high-risk conditions. Similarly, the use of big data and advanced analytics in supporting the information needs of international trade management among Ukrainian enterprises enables more accurate forecasting of foreign markets, consumer behaviour, and risks of political or economic destabilisation. The introduction and systematic use of electronic document management systems, alongside platforms such as EDI, ERP, and CRM, will greatly simplify customs clearance, customs control, logistics, and international financial settlements. In international trade, EDI, ERP, and CRM can be integrated through a unified security module that controls access, encrypts data, and monitors incidents (Table 1). Furthermore, the adoption of artificial intelligence and machine learning can facilitate automated decision-making in trade management, risk management, customer servicing, and reputation management (particularly crucial for enterprises entering foreign markets for the first time). Finally, the use of cloud technologies provides businesses with the ability to scale up the foreign economic operations significantly, without incurring substantial costs associated with developing and maintaining proprietary IT infrastructures. The challenge faced by most modern enterprises lies in the reliance on outdated management methods in providing information support for the business activities, particularly within the framework of foreign economic operations. The adoption of advanced, innovative approaches to business process management, including international trade, is not generally prioritised within the strategic development agendas. A number of enterprises are limited in utilising modern accounting information systems alone. Such an approach prevents these enterprises from promptly and comprehensively forecasting external environmental conditions – critical when entering foreign markets – planning international trade activities, evaluating the efficiency of the business processes in the context of foreign economic activity, and performing other tasks that are essential for

contemporary management in online (real-time) mode. To address these challenges, enterprises must first identify the key business processes and examine common approaches to the automation and digitalisation. The outcome of such an analysis will highlight areas requiring improvement across the enterprise as a whole. These improvements should be implemented with due regard to the specificities of its international and foreign economic operations. Effective management of such activities requires the establishment of business processes tailored to international trade conditions. In general, it is advisable to analyse the information support of economic activity, including international trade, in a systematic and staged manner. This process should begin with the identification of trade-related business processes, the allocation of points of responsibility within these processes, and the mapping of information flows that accompany international trade operations. When identifying business processes in

international trade, it is important to differentiate between universal and specialised processes. Universal trade-related processes are typically classified into the following categories: procurement of goods; value creation (formation and delivery of services, or execution of works); and sales of goods, services, or works. Specialised processes, by contrast, are enterprise-specific and relate to the management of relationships with competitive customers. Since most enterprises generally operate with a relatively limited client base, maintaining effective and sustainable communication with customers is of particular importance. Enterprises systematically engaged in foreign economic activity, and international trade in particular, continually require diverse forms of information support for the business processes, such as data on international market conditions, fluctuations in exchange rates, and modifications in customs procedures. The principal interconnections between these stages are presented in Figure 1.

Table 1. Detailed description of the use of EDI, ERP, and CRM in international trade for the development of foreign economic activity with a focus on information security

Platform names	Purpose in foreign economic activity	Characteristics of the safety aspect when using	Description of potential risks in case of insufficient protection
EDI	Automation of electronic exchange of commercial documents between partners (invoices, customs declarations, delivery notes, orders). Ensuring a unified data format in international transactions (EDIFACT, ANSI X12).	Encryption of communication channels (TLS, VPN) to protect against interception of commercial, customs, and other information. Authentication of counterparties (electronic certificates, PKI) to prevent document forgery. Audit logs to record the time, author, and content of transmitted documents. Protection against MITM attacks during international data transmission through certified EDI provider gateways.	Interception/substitution of contract data. Unauthorised access to commercial and customs information.
ERP	Centralised management of financial, logistics, production, and foreign economic activity processes. Integration with customs and transport modules for the automation of international transportation. Planning of currency transactions, warehouse stocks, and export-import schedules.	Role-based access control (RBAC) to restrict access to confidential data. Regular backups (in encrypted form) for recovery in case of cyberattacks or failures. Anomaly monitoring (detection of unauthorised changes in financial and logistical data). Integration with SIEM systems for real-time detection of security incidents.	Compromise of financial and foreign economic information, contract terms. Loss of data on inventories, delivery schedules, and other data on foreign economic transactions.
CRM	Maintaining a database of international clients and partners, tracking transaction history, communications, and correspondence. Personalised marketing campaigns for foreign markets. Communication support (email, VoIP, messengers, web forms).	Protection of customer personal data in accordance with GDPR, CCPA, and the Law of Ukraine No. 2297-VI Encryption of storage and transmission of customer contact, financial, and foreign economic information. Access control (MFA, IP filtering) to prevent unauthorised access. Detection of phishing attacks on employees who work with the international customer base.	Leaks of customer and partner data can damage reputation and even lead to fines. Use of hacked contacts for fraudulent transactions in international trade.

Source: compiled by the author based on Law of Ukraine No. 2297-VI (2010), S.P. Tron (2016), R. Lupak (2019), V. Glushchevsky *et al.* (2023), Yu. Neustroiev (2025), T. Talakh & V. Talakh (2025)

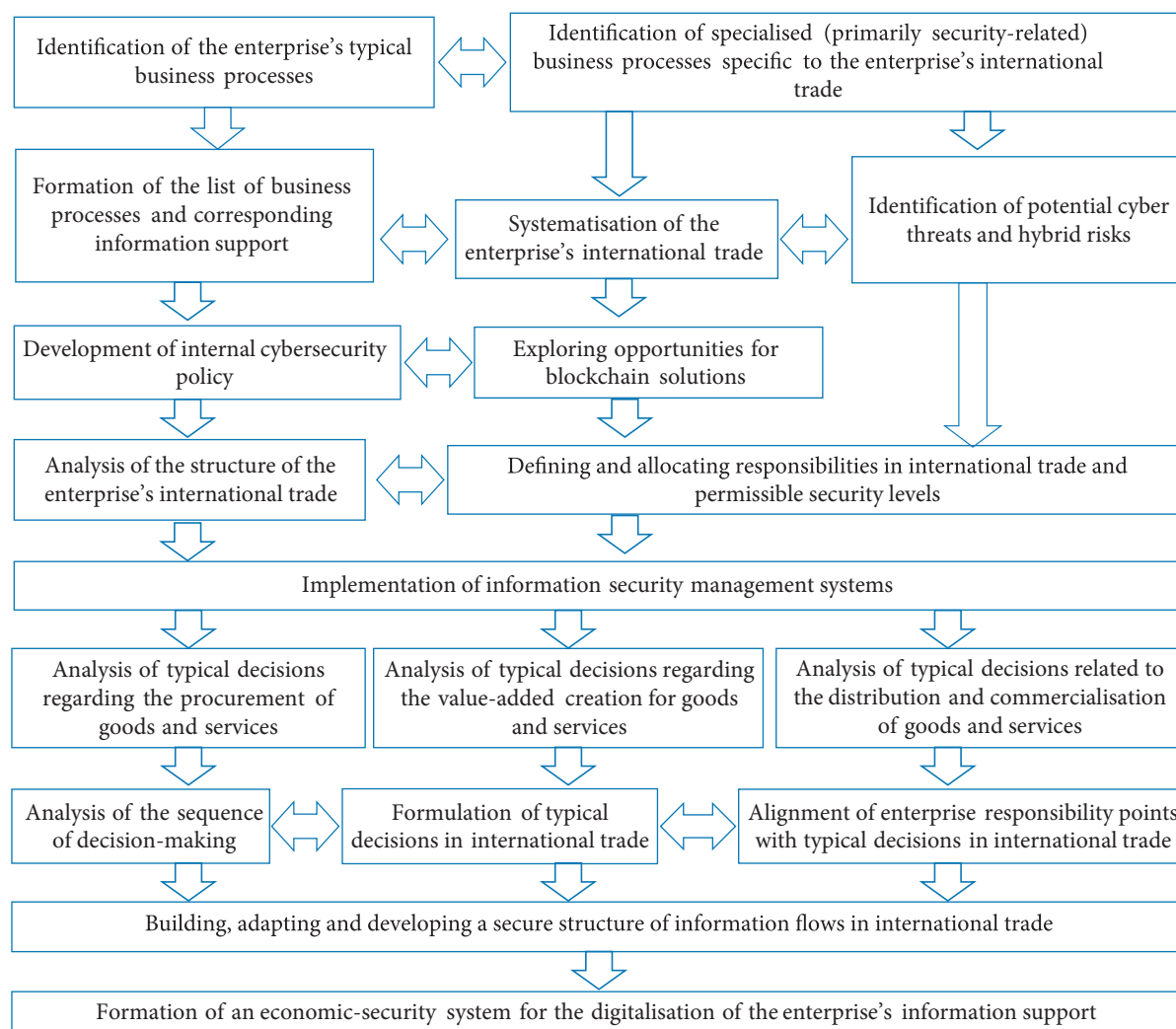


Figure 1. The recommended sequence of information support for the management of international trade by enterprises in the context of development of the foreign economic activity, taking into account the security aspect
Source: supplemented and developed based on S.P. Tron (2016), R. Lupak (2019), V. Glushchevsky *et al.* (2023)

An important element of information support for the management of international trade by enterprises in the context of the development of the foreign economic activity is the formation and implementation of information security management systems (Fig. 1). Thus, the digitalisation of information support for international trade of enterprises is the process of introducing digital technologies (primarily modern and efficient ones) into the processes of collecting, processing, analysing, storing, and transmitting data that ensure this activity of the enterprise. In foreign economic activity, digitalisation primarily covers electronic trading platforms, CRM systems, blockchain technologies (usually only for logistics, but potentially can have a much wider range of applications, as transparency and impossibility of manipulation increases the level of reliability, security, reducing risk, etc.), electronic document management, customs clearance systems, etc. Information and economic security are a set of technical, organisational, and legal measures aimed at protecting data from unauthorised

access (theft), distortion, and loss. And given the openness of the global information space and martial law in Ukraine, enterprises, entering foreign markets and operating in the market, are particularly vulnerable to digital threats. Summarising this research, systematise potential areas for ensuring the digital security of enterprises engaged in foreign economic activity, including international trade, in the current turbulent economic environment.

The formation and further development of an effective digital security system for businesses in Ukraine requires a comprehensive approach that encompasses both internal regulations and integration with international standards. The implementation and use of ISMS in accordance with international standards ISO/IEC 27001:2022 (2022) or NIST Cybersecurity Framework (n.d.) provides structured management of risks arising during the processing and storage of information. In Ukraine, Nova Poshta (n.d.) has obtained ISO/IEC 27001:2022 (2022) certification, which has enabled it to guarantee the

security of its customers' personal data and ensure the trust of its international partners. Globally, more than 44,000 organisations are certified to ISO/IEC 27001:2022 (2022), confirming the universality and effectiveness of this tool. Developing and implementing an internal cybersecurity policy that includes regular employee training, improving the digital literacy, and simulating phishing attacks is a key measure in countering social engineering. The experience of the Ukrainian banking sector, in particular PrivatBank (n.d.), shows that phishing attack simulations and online courses for employees have reduced the number of successful attacks by 68% (Table 2). According to IBM research, similar programs in global practice can reduce

this figure to 70% (Cost of a data breach report, 2025). Systematic digital audits of partner platforms and supply chains make it possible to identify weaknesses before malicious actors exploit these vulnerabilities. An alternative is blockchain technology, which ensures transparency and immutability of transactions, eliminating the need for regular audits, although it requires significant investment. The Ukrainian agricultural holding MHP is already implementing blockchain in the control of logistics operations, which reduces data verification costs by more than 15%. Similar international solutions, such as those used by Maersk (2022), have reduced data verification costs by 20% (About MHP, n.d.).

Table 2. Comparative analysis of measures for the formation and development of a digital business security system

Measures for the formation and development of a digital business security system	Examples of implementation in Ukraine	International practice	Expected effects of implementation
Implementation of ISMS in accordance with ISO/IEC 27001:2022, NIST CSF	Nova Poshta is certified according to ISO/IEC 27001:2022 for the protection of personal data and partner trust	Over 44,000 organisations are certified according to ISO/IEC 27001:2022	Reduced risk of data leaks, increased reputational resilience
Internal cybersecurity policy with staff training and phishing attack simulations	PrivatBank reduced the success rate of attacks by 68% through training and phishing simulations	IBM: staff training reduces the success rate of attacks by 70%	Minimisation of the human factor, reduction of social engineering threats
Digital audit of partners and supply chains / blockchain technology	MHP implements blockchain in logistics control, reducing costs by 15%	Maersk reduced data verification costs by 20% due to blockchain	Transparency of supply chains, early detection of vulnerabilities
Use of modern security measures (MFA, encryption, NGAV, monitoring)	SoftServe implemented MFA, which prevented 95% of unauthorised access attempts	Microsoft: MFA blocks 99% of automated attacks	Increased cyber resilience, reduced number of incidents
Participation in national and international cybersecurity programs	Cooperation between IT companies and ECSO for information exchange and solution testing	The Digital Europe program funds cyber projects and data exchange	Access to technologies, coordinated response mechanisms
Single incident response centre	The State Centre for Cyber Protection of the State Special Communications Service reduces response time from days to hours	CERT-EU reduces incident resolution time through centralisation	Rapid detection, quick neutralisation of threats

Source: developed based on State Service of Special Communications and Information Protection of Ukraine (n.d.), PrivatBank (n.d.), About MHP (n.d.), IIEA (n.d.), ISO/IEC 27001:2022 (2022), Maersk (2022), SoftServe (2024), Microsoft digital defence report 2024 (2024), Cost of a data breach report (2025), CERT-EU (2025)

The systematic use of modern information security measures – multifactor authentication (MFA), data encryption, the latest antivirus platforms with regular updates, and user activity monitoring – significantly increases companies' cyber resilience. The Ukrainian IT company SoftServe (2024) has implemented multifactor authentication on all internal services, which has prevented over 95% of unauthorised access attempts. The Microsoft digital defence report 2024 (2024) confirmed that MFA blocks over 99% of automated attacks.

Participation in national and international cybersecurity programs, particularly within the framework of integration into the EU digital market, provides access to advanced technologies and coordination mechanisms for response. An example is the cooperation between Ukrainian IT companies and the European Cyber Security

Organisation (ECSO, n.d.), which allows for the exchange of information about threats and joint testing of new security measures (IIEA, n.d.). The creation of a single incident response centre ensures the rapid detection and localisation of cyber threats. In Ukraine, this function is partially performed by the State Cyber Protection Centre State Special Communications (2024), which cooperates with private entities to reduce the response time to incidents from several days to several hours. The similar experience of CERT-EU (2025) in the European Union confirms the effectiveness of a centralised response. The security aspect of digitalisation of information support for international trade of enterprises is extremely important. After all, it is security challenges and threats that are the determining barriers to the digital transformation of foreign economic activity, including international trade of enterprises.

The main areas of security include: cyber hygiene for staff; training employees to recognise phishing and social engineering attacks; implementation of ISO/IEC 27001 and NIST CSF standards in information security management systems; two-factor authentication, encryption, and user activity monitoring; creation of a single incident response centre (CERT) at the enterprise or industry level.

It is advisable for businesses to carry out digital transformation. This should be done taking into account the principle of “security by default”. This is absolutely justified under martial law, but it can also be used in the post-war period of recovery and revival. Contracts with foreign partners of Ukrainian companies should necessarily include a provision (clause) on data/information protection. It may also be advisable to create information security departments (costly and ineffective for small businesses), and to engage external cybersecurity specialists (on an outsourcing basis). Expanding the access of businesses (its entities) to state digital platforms (in particular, Diia.Business, the Single Window for International Trade, etc.) should be accompanied by strengthening security protocols at the global (national/state) level, etc.

Discussion

A. Drabovskiy (2025) research emphasised the importance of addressing cybersecurity and data protection (as an integral part of a digital transformation strategy that helps reduce risks and increase trust in innovative solutions). And it is effective resistance management (Tomashkov & Oherchuk, 2023; Drabovskiy, 2025) that is a critical factor in the processes of introducing new technologies and management methods. By overcoming internal barriers, an organisation can achieve high competitiveness in the digital economy. It was worth agreeing with A. Drabovskiy (2025) that in order to ensure sustainable development and modernisation of an enterprise, it is necessary to implement comprehensive strategies focused on continuous improvement, innovation, and adaptive management, which allow responding to modern challenges and effectively utilising the potential of digital technologies. V. Tsopa (2023) carried out a detailed risk assessment in the studies. The authors of the present study agreed with V. Tsopa (2023) that risk (in all spheres of life) is inherent in every process and, under market conditions, is linked to the results of economic activity. V. Tsopa (2023) clearly defined the conceptual framework of risk, in particular the causes, consequences, and objects of risk.

In the research, O. Lyzunova *et al.* (2025) noted that the use of digital technologies allows enterprises to optimise the processes of documenting foreign trade operations, reduce the risks of errors and fraud, and ensure compliance with international standards. However, O. Lyzunova *et al.* (2025) narrowed the research to the field of accounting. It is worth agreeing with O. Lyzunova *et al.* (2025) that the intensification of innovation contributes to improving the quality of analytical information used for management decision-making, reducing the time required to process large

amounts of data, and facilitating the monitoring of financial flows and interaction with counterparties from different countries. O. Lyzunova *et al.* (2025) linked the future of digitalisation of foreign economic activity with the widespread use of artificial intelligence and big data, which will increase the accuracy of forecasting and automate decision-making. Process automation, transparency, and speed of work significantly increase the efficiency of foreign economic activity management. Scientists point out that successful digitalisation will allow enterprises not only to adapt to modern conditions, but also to become leaders in the industries.

Yu. Neustroiev (2025) stated in the research that economic security is a dynamic state (which is constantly influenced by numerous variables) and requires the systematic application of specialised criteria, indices, and indicators capable of accurately reflecting the state of economic stability and risks, as well as vulnerability factors. Similar views were presented in a study by A. Tkachenko & D. Mezheryskyi (2023) where the authors emphasised that strengthening economic protection mechanisms is a necessary condition for maintaining business sustainability and stability in conditions of uncertainty. This is consistent with this research. Yu. Neustroiev (2025) also argued that innovation is an effective tool for ensuring a country's economic security, as it can significantly increase competitiveness in the international market. This is a reasonable conclusion. The author also pointed out that it is innovation that initiates the development of socially responsible business, contributes to the prosperity of individual enterprises and local communities, and creates conditions for strengthening the national economy. This was confirmed by global practice. While innovation plays a decisive role in the development of developed countries' economies, it is also necessary to take into account that some innovations can have negative environmental consequences, which must be calculated and balanced within the framework of economic security.

E-commerce constitutes a significant share of international trade, and this component demonstrates a steady growth trend. The issues of e-commerce are addressed in the works of A.U. Rehman *et al.* (2022) and S. Kniaz *et al.* (2023). The authors' definition of the characteristics of e-commerce in relation to warranty servicing and customer support was considered accurate. The authors of this scientific study quite reasonably proposed that, in order to improve the system of servicing and warranty support for consumers in the field of e-commerce, it is advisable to implement a customer loyalty programme; enhance the qualifications of personnel (particularly employees of service centres); improve delivery services through high-quality packaging of goods by applying innovative solutions; and introduce the option of payment upon delivery for purchased goods (as an element of strengthening economic security and corporate reputation).

An important achievement is the mechanism proposed by I. Rudenko (2023) for integrating logistics marketing and information management into the strategic development of enterprises. The structure of the mechanism

provides for the inclusion of a marketing module, an information management module, analytics and control, a logistics module, and a customer service module. It is worth agreeing with the author I. Rudenko (2023) that the implementation of this mechanism will enable the enterprise to achieve strategically important results, in particular: reduction of production costs, increase in customer loyalty (especially international customers), increasing the flexibility of the supply chain, and ensuring a quick response to changes in the markets (domestic and foreign). H. Anishchenko *et al.* (2025) analysed the system of accounting and information-analytical support for managing the process of restoring the resource potential of agricultural enterprises, which constitutes an important element in the implementation of information technologies in international trade. This interpretation was considered valid. In the study, M.S.A. Alsheyab (2025) examined the advantages of electronic transferable records as a step towards the digitalisation of cross-border trade. This represents a crucial component of the digitalisation of international trade in conjunction with the domain of security. It is essential to emphasise the importance of digitalisation as a driving force for the sustainable development of enterprises within the European vector (Blakytta *et al.*, 2025). The validity of this element is acknowledged for the effective advancement of the digitalisation of international trade, as it contributes significantly to the sphere of security in the implementation of international trade.

M. Blikhar *et al.* (2023) investigated shadow economy vs economic security: trends, challenges, prospects. Fully agree with the close interconnection of these factors. The results of the study of the dynamics of the integral indicator of the shadow economy and changes in real GDP in Ukraine are important, and the volume of official GDP created by shadow wages has been estimated. Forecasts of the shadow economy and poverty levels for the coming years have been made, and growth trends have been identified. It has been established that the growth of the shadow economy has a significant impact on the poverty rate of the population. M. Bortnikova & S. Slipachuk (2025) analysed improvement of new management technologies implementation at enterprises in the conditions of foreign economic activity in the research. The proposed reengineering implementation technology is quite relevant in scientific work. It provides an opportunity to carry out comprehensive preparation for the implementation of business processes, to assess the feasibility of introducing a new mechanism in terms of identifying the costliest measures and the safety of the application. And it is the implementation of reengineering that is a strategic decision that will increase the efficiency, competitiveness, and adaptability to changes of Ukrainian business. This is important in the context of European integration and the expansion of foreign trade.

Key factors of the impact of digitalisation on entrepreneurship were reflected in the work of V. Glushchovsky *et al.* (2023), highlighting the importance and significance. The conducted study demonstrated the impact of

economic digitalisation on entrepreneurship, reshaping the business landscape and opening new opportunities for entrepreneurs. The analysis of factors influencing entrepreneurship in the course of economic digitalisation, with due consideration of security aspects, provided a deeper understanding of these transformations and the implications for business, including international business. Among the key factors identified in this research were technological progress, the spread of digital technologies, shifts in consumer behaviour, e-commerce, globalisation, and transformations in business models. This recognition of influential factors underlined the necessity of a structured approach for entrepreneurs seeking to leverage digital opportunities. Of particular importance is the recognition of the influence of these factors on the modern business environment, enabling entrepreneurs to adapt to new conditions. A significant outcome of the study was the proposed classification system of the examined factors, based on two criteria: the type of interaction with enterprises (internal and external), and the sphere of influence (technological, socio-economic, and organisational). Such classification provided a clear framework for understanding challenges and opportunities arising from economic digitalisation, supporting more informed strategic decisions.

Scientific works on managing the risks of introducing information technologies into international trade in the development of foreign economic activity are also important. This was reflected in the studies of K. Hrabina & V. Shendryk (2023), which indicated that, in order to ensure management efficiency, it is advisable to apply risk management of IT projects with due consideration of threats and opportunities. In this context, risk management becomes an integral part of enterprise strategy under conditions of global digitalisation. The assertion of O. Melnyk & D.-I. Yakymets (2025) that the establishment of a risk management system constitutes a key factor in the successful integration of Ukrainian enterprises into the European economic space is valid. The development and implementation of a risk management framework for the foreign economic activity of enterprises under conditions of European integration – based on the application of advanced tools for risk identification, assessment, and optimisation – should be considered a strategic priority for enterprises seeking success in global European markets. The importance of forming a risk management system during the implementation of information technologies in international trade when developing foreign economic activity was also emphasised by U. Savkiv *et al.* (2022). Taken together, these studies highlighted the centrality of risk frameworks in ensuring stability and competitiveness for enterprises operating in international markets.

Micro-level issues have not been sufficiently researched, as noted in the works of B. Ilychok *et al.* (2024). The authors demonstrated that the dynamics of the shadow economy indicators in Ukraine are inconsistent with the goals and objectives of the Economic Security Strategy of Ukraine for the period up to 2025. Addressing these

inconsistencies is critical for enhancing monetary policy and reinforcing state governance. The measures proposed for minimising the negative factors of influence provide a basis for improving the implementation of monetary policy and enhancing the effectiveness of state governance in ensuring Ukraine's currency security. O. Likhota (2025) had examined the impact of international cooperation, particularly with the EU, and identified relevant factors for consideration in the formulation of economic security policy. I. Nazarova (2023) noted that developers of international regulatory frameworks strive to keep pace with economic progress by expanding the scope of the concept of the electronic document, resulting in international interpretations that are better aligned with contemporary standards of partnership relations, without requiring visual legibility for human perception or attachment to a physical medium. These findings emphasised the interconnectedness of international cooperation, regulatory adaptation, and enterprise security in the context of global digitalisation. The challenges of introducing information technologies into international trade were highlighted in the works of O. Kibik *et al.* (2022). The interpretation regarding the use of modern e-commerce methods, digital platforms, and blockchain to provide companies with new advantages and opportunities is timely and valid. Integrating these innovations into enterprise strategy allows for both immediate gains and long-term competitiveness. Enterprises adopting a strategic development approach that combines innovative methods, analysis of internal and external resources, and adequate adaptation to the realities of the digital economy achieve significant results. Organisations such as the European Commission, and coordinating bodies such as the Steering Committee for the Implementation of the e-Government Action Plan, play a crucial role in creating a forum for engaging all key stakeholders, with the participation of private legal entities ensuring market adoption of outcomes (Schmidt & Krimmer, 2022).

The importance of information provision as an element of enhancing the economic security of enterprises was also emphasised by T. Talakh & V. Talakh (2025). Properly structured information channels become a backbone for informed decision-making and risk management. The application of advanced European experience in the implementation of information technologies in international trade in the development of foreign economic activity is significant in Ukraine, as reflected in the works of C. Schmidt & R. Krimmer (2022) and T. Zubko *et al.* (2021). Based on modelling, a statistically significant correlation has been identified between the indicators of information volume and related services, and the volumes of trade, confirming the dependence of economic security of trading enterprises on digitalisation. The proposal to complement the existing methodology for assessing the economic security of trading enterprises with indicators reflecting the impact of digital technologies is particularly important. This approach ensured that evaluation frameworks remain relevant in a rapidly evolving digital business environment.

The development of Economy 4.0 as an element of trade digitalisation, including international trade, is analysed in V. Makedon & O. Mykhailenko (2024). The impact of Economy 4.0 on global logistics operations of transnational corporations highlighted its relevance for the implementation of information technologies in international trade, although the security aspect remains unaddressed. Global crises, such as the COVID-19 pandemic, armed conflicts, and climate change, significantly impact logistics, leading to declines in international trade indicators. Wars, such as the war in Ukraine, increase costs and delivery times, while heightening risks of loss or damage due to the necessity of bypassing conflict zones. Climate-related challenges exacerbate risks associated with freight transport. In response, modern transnational corporations adopt innovative solutions to enhance customer convenience, optimise delivery routes, and track cargo efficiently. Investment in innovations aimed at modernising logistics is steadily increasing, providing considerable competitive advantage to actively investing corporations. Despite significant achievements in researching the implementation of information technologies in international trade, the security aspect remains somewhat overlooked in the development of foreign economic activity.

Conclusions

The analysis of the choice, implementation and further use of IT in the activities of enterprises revealed a number of problems/threats to the use of IT, the specifics of the application, etc. The main ways to solve (resolve) these problems should be the following: changing the traditional outdated information system at enterprises; convincing the management (especially the top management) of the urgent need to invest in modern IT systems for managing strategic potential through a feasibility study; clearly defining strategic and tactical goals and objectives of the IT system of enterprises; developing and using an effective system for managing the strategic potential of enterprises, taking into account digital transformation, enhancing the level of information security, integrating innovative technologies, and fostering an adaptive organisational culture capable of ensuring sustainable development in a dynamic competitive environment. Enterprise information technologies have become high-speed virtual machines for solving various issues, including in international trade. By actively and systematically using IT technologies, Ukrainian enterprises will be able to increase the competitiveness, as well as the competitiveness of goods sold, services provided, and work performed.

A comparative analysis of measures to establish and develop a digital business security system has revealed positive and effective results in Ukraine, namely: Nova Poshta is certified according to ISO/IEC 27001 for the protection of personal data and partner trust; PrivatBank reduced the success rate of attacks by 68% through training and phishing simulations; MHP implements blockchain in logistics control, reducing costs by 15%; SoftServe implemented MFA, which prevented 95% of unauthorised access

attempts. With regard to foreign experience, it can be stated that over 44,000 organisations are certified according to ISO/IEC 27001; IBM: staff training reduces the success rate of attacks by 70%; Maersk reduced data verification costs by 20% due to blockchain; Microsoft: MFA blocks 99% of automated attacks. In general, for the effective functioning of an enterprise (not only in the context of foreign economic activity), it needs to form a secure information system that would be able to meet all the complex needs of the enterprise for a long time. Given the dynamism of the global economic environment, security aspects, the growing role and importance of the use of digital technologies in foreign economic activity (in particular, international trade), further research should be directed to the following areas: assessing the level of effectiveness of digital solutions in foreign economic activity; detailing and analysing the impact of specific information technologies (ERP systems,

blockchain platforms, electronic identification systems, etc. to increase the operational efficiency of international trade of enterprises; formation of the digital ecosystem of international trade of Ukraine; research of the possibilities of creating integrated national, sectoral IT platforms, IT clusters to coordinate export-import activities, taking into account the world practices of digital regulation; modelling the risks of cyber threats in international trade, etc.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

- [1] About MHP. (n.d.). Retrieved from <https://mhp.com.ua/uk/pro-kompaniiu>.
- [2] ALsheyab, M.S.A. (2025). Legal analysis of the merits of electronic transferable records: Toward cross-border trade digitalization. *International Journal of Law and Management*, 67(1), 145-163. doi: 10.1108/IJLMA-09-2023-0209.
- [3] Anishchenko, H., Pidlubna, O., & Basok, A. (2025). Accounting, information, and analytical support for managing the process of restoring the resource potential of agricultural enterprises. *Efficient Economy*, 7. doi: 10.32702/2307-2105.2025.7.85%20.
- [4] Blakyt, H., Bagatska, K., & Susidenko, V. (2025). Digitalization as a driver of enterprise sustainability in the European vector. *Business Inform*, 2, 135-142. doi: 10.32983/2222-4459-2025-2-135-142.
- [5] Blikhar, M., Syrovatskyi, V., Bek, U., Vinichuk, M., Kucher, L., & Kashchuk, M. (2023). Shadow economy vs economic security: Trends, challenges, prospects. *Economic Studies*, 32(3), 130-147. doi: 10.13140/RG.2.2.24624.23049.
- [6] Bortnikova, M., & Slipachyk, S. (2025). Improvement of new management technologies implementation at enterprises in the conditions of foreign economic activity. *Management and Entrepreneurship in Ukraine: Stages of Formation and Problems of Development*, 5(2), 27-34. doi: 10.23939/smeu2025.02.027.
- [7] Bulavynets, O. (2025). The current state of social transfers: Digitalization and inclusiveness. *Business Inform*, 2, 156-162. doi: 10.32983/2222-4459-2025-2-156-162.
- [8] CERT-EU. (2025). *Threat landscape report 2024: A year in review*. Retrieved from <https://www.cert.europa.eu/publications/threat-intelligence/tlr2024/pdf>.
- [9] Cost of a data breach report. (2025). Retrieved from <https://www.ibm.com/reports/data-breach>.
- [10] Drabovskyi, A. (2025). Innovative strategies for managing organizations in the context of digital transformation. *Efficient Economy*, 4. doi: 10.32702/2307-2105.2025.4.4.
- [11] ECSO. (n.d.). Retrieved from <https://ecs-org.eu/>.
- [12] Glushchevsky, V., Holomb, V., & Byrskyi, V. (2023). The impact of digitalization on entrepreneurship: Key factors. *Humanities Studies*, 16(93), 160-167. doi: 10.32782/hst-2023-16-93-16.
- [13] Hrabina, K., & Shendryk, V. (2023). Method of the risk management of IT projects taking into account threats and opportunities. *Management of Development of Complex Systems*, 55, 18-28. doi: 10.32347/2412-9933.2023.55.18-28.
- [14] IIEA. (n.d.). *Digital*. Retrieved from https://www.iiea.com/digital?gad_source=1&gad_campaignid=22339636043&gbraid=0AAAAAD30q8AVhDNm9N0fR19xDedl4yFuh&gclid=Cj0KCQjwqebEBhD9ARIsAFZMbf8mAlXUIOLR0q-bNqPKMYVsBS_XVcG512jEZTYpSEDLmfogtnR3saAnJ4EALw_wcB.
- [15] Ilychok, B., Dziurakh, Y., Karkovska, V., Kucher, A., Marmulyak, A., & Tsyarkin, A. (2024). Public management of currency security in Ukraine: Challenges and perspectives in modern realities. *Financial and Credit Activity Problems of Theory and Practice*, 3(56), 308-320. doi: 10.55643/fcaptp.3.56.2024.4311.
- [16] ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection – information security management systems – requirements*. Retrieved from <https://www.iso.org/standard/27001>.
- [17] Kibik, O., Taran-Lala, O., Saienko, V., Metil, T., Umanets, T., & Maksymchuk, I. (2022). Strategic vectors for enterprise development in the context of the digitalization of the economy. *Postmodern Openings*, 13(2), 384-395. doi: 10.18662/po/13.2/460.
- [18] Kniaz, S., Heorhiadi, N., Kucher, L., Tyrkalo, Yu., & Bovsunivska, A. (2023). Development of a customer service system in electronic commerce. *Business Management*, 2, 64-82. doi: 10.58861/tae.bm.2023.2.04.

- [19] Law of Ukraine No. 1089-IX "On Electronic Communications". (2020, December). Retrieved from <https://zakon.rada.gov.ua/laws/show/1089-20#Text19>.
- [20] Law of Ukraine No. 1789-VIII "On Information". (1992, October). Retrieved from <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
- [21] Law of Ukraine No. 2155-VIII "On Electronic Identification and Electronic Trust Services". (2017, October). Retrieved from <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.
- [22] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
- [23] Law of Ukraine No. 675-VIII "On Electronic Commerce". (2015, September). Retrieved from <https://zakon.rada.gov.ua/laws/show/675-19#Text>.
- [24] Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management". (2003, May). Retrieved from <https://zakon.rada.gov.ua/laws/show/851-15#Text>.
- [25] Likhota, O. (2025). Legislative support of the US information policy. *Economics. Finances. Law*, 3, 65-68. doi: 10.37634/efp.2025.3.12.
- [26] Lupak, R. (2019). Directions for realization of the potential of the information and communication technologies sector in the context of ensuring the quality characteristics of the internal market and the development of the information society in Ukraine. *Galician Economic Herald*, 60(5), 79-94. doi: 10.33108/galicianvisnyk_tntu2019.05.079.
- [27] Lyzunova, O., Lysenko, S., & Prydatko, E. (2025). Implementation of digital technologies in the accounting of foreign economic activity of the enterprise. *Economic Space*, 199, 71-75. doi: 10.30838/EP.199.71-75.
- [28] Maersk. (2022). *A.P. Moller-Maersk and IBM to discontinue TradeLens, a blockchain-enabled global trade platform*. Retrieved from <https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens>.
- [29] Makedon, V., & Mykhailenko, O. (2024). Impact of economy 4.0 on global logistics operations of transnational corporations. *Economic Space*, 189, 276-282. doi: 10.32782/2224-6282/189-49.
- [30] Melnyk, O., & Yakymets, D.-I. (2025). Features of risk management of foreign economic activities of enterprises in the conditions of European integration. *Economics. Finances. Law*, 3, 114-117. doi: 10.37634/efp.2025.3.21.
- [31] Microsoft digital defence report 2024. (2024). Retrieved from <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024>.
- [32] Nazarova, I. (2023). Electronic document in the context of international economic and legal relations. *Journal of European Economics*, 22(1), 33-48. doi: 10.35774/jee2023.01.031.
- [33] Neustroiev, Yu. (2025). *Innovative development in the observance of economic security of sectoral and territorial economic systems and complexes*. (Doctoral dissertation, Odesa National University of Technology, Odesa, Ukraine).
- [34] NIST Cybersecurity Framework. (n.d.). Retrieved from <https://www.nist.gov/cyberframework>.
- [35] Nova Poshta. (n.d.). Retrieved from <https://novaposhta.ua/en/>.
- [36] PrivatBank. (n.d.). Retrieved from <https://privatbank.ua/en>.
- [37] Rehman, A.U., Bashir, S., Mahmood, A., Karim, H., & Nawaz, Z. (2022). Does e-shopping service quality enhance customers' e-shopping adoption? An extended perspective of unified theory of acceptance and use of technology. *PLoS ONE*, 17(2), article number e0263652. doi: 10.1371/journal.pone.0263652.
- [38] Rudenko, I. (2023). The information technology market as a driver of post-war recovery. *Foreign Trade: Economics, Finance, Law*, 128(3), 67-82. doi: 10.31617/3.2023(128)06.
- [39] Savkiv, U., Sydor, H., & Tymkiv, A. (2022). Risk management of foreign economic activity of enterprises in wartime. *Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas (Series: Economics and Management in the Oil and Gas Industry)*, 2(26), 79-88. doi: 10.31471/2409-0948-2022-2(26)-79-88.
- [40] Savras, I.Z., & Fedynets, V.I. (2023). Digitalisation and innovative development of the enterprise: Trends, challenges and prospects. *Herald of Lviv University of Trade and Economics. Economic Sciences*, 74, 108-114. doi: 10.32782/2522-1205-2023-74-14.
- [41] Schmidt, C., & Krimmer, R. (2022). How to implement the European digital single market: Identifying the catalyst for digital transformation. *Journal of European Integration*, 44(1), 59-80. doi: 10.1080/07036337.2021.2011267.
- [42] SoftServe. (2024). *Service organization controls (SOC) 3 report*. Retrieved from <https://surl.it/xixvhk>.
- [43] State Service of Special Communications and Information Protection of Ukraine. (n.d.). Retrieved from <https://cip.gov.ua/en>.
- [44] Talakh, T., & Talakh, V. (2025). Features of the methodology for analyzing trade enterprises and its information support. *Economy and Society*, 71. doi: 10.32782/2524-0072/2025-71-11.
- [45] The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine (SCPC SSSCIP) is increasing technical capabilities of the National Center for Reserving State Information Resources. (2024). Retrieved from <https://scpc.gov.ua/en/articles/366>.
- [46] Tkachenko, A., & Mezheryskyi, D. (2023). *The role of economic security as a tool for ensuring business stability*. *Management and Business*, 1(2), 128-140.

- [47] Tomashkov, S.B., & Oherchuk, Yu.V. (2023). Assessment of the impact of risks of foreign economic activity. *Management and Entrepreneurship in Ukraine: The Stages of Formation and Problems of Development*, 5(2), 142-151. doi: 10.23939/smeu2023.02.142.
- [48] Tron, S.P. (2016). *Analysis of information support of trade enterprises*. *Uzhorod National University Herald. Series: International Economic Relations and World Economy*, 7(3), 135-138.
- [49] Tsopa, V. (2023). *Identification and classification of risks*. Retrieved from <https://qualityexpert.com.ua/interviews/657215-identyfikatsiya-i-klasyfikatsiya-ryzykiv>.
- [50] Vasylytsiv, T., Lypak, R., & Vasylytsiv, V. (2017). *Analysis of macroeconomic, industrial, financial, intellectual and human resources component of Ukraine information and communication technologies sector security*. *The Economic Discourse*, 1, 161-172.
- [51] Zaverbnyi, A., Zalizna, L., & Trach, M. (2024). Digitalization as an important factor in the formation of the competitiveness of an export-oriented enterprise: An information aspect. *Economy and Society*, 60. doi: 10.32782/2524-0072/2024-60-19.
- [52] Zubko, T., Hanechko, I., Trubei, O., & Afanasyev, K. (2021). Determining the impact of digitalization on the economic security of trade. *Eastern European Journal of Enterprise Technologies*, 6(13(114)), 60-71. doi: 10.15587/1729-4061.2021.248230.

Впровадження інформаційних технологій у міжнародну торгівлю при розвиванні зовнішньоекономічної діяльності: безпековий аспект

Андрій Завербний

Доктор економічних наук, професор
Національний університет «Львівська політехніка»
79013, вул. Степана Бандери, 12, м. Львів, Україна
<https://orcid.org/0000-0001-7307-536X>

Анотація. Метою статті було дослідження та розвиток інформаційного забезпечення управління міжнародною торгівлею українськими підприємствами за умов розвивання їх зовнішньоекономічної діяльності із врахуванням безпекового аспекту. Теоретико-методологічні основи даного дослідження базувалися на застосуванні комплексного міждисциплінарного підходу, котрий ефективно поєднав економічну теорію міжнародної торгівлі, інформаційну і економічну безпеки, управління ризиками, цифрове трансформувannya. Основними методами виступали: системний аналіз, порівняльне дослідження, аналізування цифровізування. Проведено огляд літературних джерел та правової бази за проблематикою запровадження інноваційних інформаційних технологій у міжнародну торгівлю українських підприємств, їх безпековий аспект. У роботі зазначено, що безпековий аспект цифровізування інформаційного забезпечення міжнародної торгівлі українських підприємств має суттєве значення. Саме безпекові виклики та загрози виступають визначальними бар'єрами для цифрового трансформувannya зовнішньоекономічної діяльності, зокрема міжнародної торгівлі підприємств. Розкрито особливості використання інформаційних технологій у зовнішньоекономічній діяльності, зокрема в контексті цифрового трансформувannya, кібербезпеки, регуляторної відповідності. Окреслено перспективи, що відкриваються завдяки інтегруванню цифрових рішень, таких як електронні платформи, блокчейн, big data, штучний інтелект. Розроблено пропозиції щодо підвищення рівня інформаційної безпеки в умовах глобалізування, цифровізування світових торговельних відносин. Запропоновано послідовність інформаційного забезпечення управління міжнародною торгівлею українськими підприємствами за умов розвивання їх зовнішньоекономічної діяльності із врахуванням безпекового аспекту. Визначено інформаційні системи, які є здатними оцінювати конкурентне середовище, враховувати всі важливі для підприємств макроекономічні, інституційні, мікроекономічні, безпекові та інші фактори ринку, вимірювати, оцінювати, прогнозувати конкуренцію в галузі, в країні, в регіоні, технологічне відставання, потреби клієнтів (передусім це стосується нових, при виході на іноземні ринки), замовників. Встановлено, що для забезпечення ефективної роботи підприємства, зокрема в умовах зовнішньоекономічної діяльності, необхідно створити надійну інформаційну систему, здатну тривалий час задовольняти комплексні потреби підприємства

Ключові слова: цифровізація; глобалізація; економічна безпека; інформація; кібербезпека