SECTION 3
Methodological framework for ensuring socio-economic security through digital transformation of the economy

ANDROSOV Volodymyr,
PhD candidate (third level of higher education)
in the field of knowledge
05 "Social and Behavioral Sciences", specialty 051 "Economics",
Zaporizhzhia National University,
Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0009-0009-3358-9361

3.1. MODERN RESPONSE TECHNOLOGIES AND THREATS TO NATIONAL SECURITY

Introduction. Ensuring Ukraine's national security is a top priority for the state amidst a complex and dynamic geopolitical environment. The ongoing armed conflict, hybrid threats, and cyberattacks require constant search for and implementation of innovative approaches and tools to protect sovereignty, territorial integrity, and citizens. In this context, modern technologies play a key role, offering unprecedented opportunities to strengthen the country's defense capabilities, detect and neutralize threats at early stages, and respond effectively to crises.

This study provides a comprehensive analysis of the use of advanced technologies in the field of national security in Ukraine, examines the main threats facing the state, and assesses the potential of technologies in ensuring resilience and safety. Special attention is given to key technologies and recommendations for further strengthening Ukraine's national security through technological innovation.

Presentation of Key Research Findings. In the context of ongoing military actions, several modern technologies are actively employed in the service of Ukraine's national security. Artificial intelligence (AI) and machine learning are becoming increasingly important tools in this domain. These technologies offer considerable potential for analyzing large volumes of data to detect threats, automate decision-making processes, and support military operations [1]. Machine learning algorithms can be used to identify anomalies in network traffic – potential indicators of cyberattacks – or to analyze satellite imagery for signs of suspicious activity along borders.

The advancement of generative AI introduces new possibilities, including the creation of realistic training simulations for military personnel and the development of intelligent decision support systems [2]. However, it is important to note that adversaries may also leverage generative AI to produce more convincing disinformation campaigns and phishing attacks. On a global scale, there is increasing competition among states for leadership in AI development, emphasizing the strategic significance of this technology for national security [4].

Quantum technologies, particularly quantum computing, have the potential to revolutionize numerous fields, including national security. Quantum computers could significantly accelerate complex computations, useful for cryptography, material science, and big data analysis. At the same time, the development of quantum computing poses a threat to existing encryption systems, as these computers could theoretically break many current cryptographic algorithms. Advancing quantum technologies requires substantial investment in research and development, with major tech companies playing a key role due to their financial and scientific capabilities.

International cooperation in the field of quantum technologies is also crucial for ensuring national security, as no single country can independently cover the full scope of research in this area [4].

Biotechnologies have a broad range of applications relevant to national security, including the development of new medical treatments and vaccines, the creation of biosensors for threat detection, and the use of biological processes in industry and agriculture.

However, the advancement of biotechnology also carries risks, such as the potential creation of biological weapons and the threat of bioterrorism. Rapid progress in biotechnology – especially when combined with artificial intelligence – may lead to unforeseen consequences for national security. Increasing competition among major global powers in this field further highlights the strategic importance of biotechnology [2; 4].

Unmanned systems, particularly drones, have become indispensable tools for intelligence gathering, surveillance, strike operations, and logistical support in military contexts. Drones can be used for border monitoring, detection of illegal activity, counter-terrorism operations, and assessment of disaster consequences. At the same time, there is a growing threat of terrorist groups using drones to carry out attacks. This makes the development of counter-drone technologies–such as detection, interception, and neutralization systems–increasingly vital. The lack of a clear national strategy for drone use and regulation may pose a significant threat to national security [4].

Satellite technologies are critically important for communication, navigation, intelligence, and surveillance in support of national security. Satellites are used to collect intelligence, monitor borders, ensure communication between military units, and provide navigation services. A key aspect is ensuring the resilience of satellite systems against cyberattacks and physical threats, as their failure can have serious implications for national security. The growing number of small satellites is making space technology more accessible, but also complicates oversight of their potential military use. The private sector is playing an increasingly important role in satellite technology development, which may affect state control in this strategically vital area [4].

Cybersecurity technologies are a crucial element in protecting national interests in the digital space. A wide range of technologies and systems – including intrusion detection systems, firewalls, antivirus software, threat detection and response systems, as well as encryption and biometric authentication technologies – are used to defend against cyber threats. Artificial intelligence plays an increasingly important

role in enhancing cybersecurity by helping detect anomalies, predict attacks, and automate response processes.

Cyber threats are becoming more complex and diverse, including attacks on critical infrastructure, ransomware, and phishing campaigns. Effectively countering these threats requires close international cooperation and information sharing on cyber incidents [4; 5].

Artificial intelligence has proven highly effective in identifying potential national security threats by analyzing large volumes of data. Machine learning algorithms can detect anomalies in network traffic that may indicate a cyberattack, or recognize patterns in video and photo imagery to help identify suspicious individuals or objects. AI systems can analyze data from various sources, including social media and open-source platforms, to detect signs of planned terrorist activities or the spread of disinformation.

Satellite imagery and remote sensing data are also used to monitor borders, detect illegal activities such as arms or drug smuggling, and assess the impact of natural disasters and technological accidents. AI plays a key role in processing and analyzing this data, helping identify patterns and anomalies that may indicate potential threats. However, it should be noted that adversaries are also actively using AI to enhance their attack methods, which necessitates the ongoing development and adaptation of threat detection systems [1; 7].

Preventing national security threats is just as important as detecting and responding to them. In the field of cybersecurity, this is achieved through the implementation of comprehensive protection systems, including the use of firewalls, intrusion detection systems, data encryption technologies, and multi-level authentication, including biometric methods. At the borders, biometric technologies are employed to identify individuals and monitor their movement, helping to prevent the entry of persons who may pose a threat. Unmanned aerial vehicles are used to patrol borders and detect illegal crossings, smuggling, and other illicit activities. The effectiveness of these measures depends not only on the availability of modern technologies but also on their proper implementation, continuous monitoring and timely updating, as well as the training level of personnel responsible for their operation [8].

In the event of a national security threat, modern technologies provide tools for rapid and effective response. Unmanned systems can be quickly deployed to assess the situation, conduct search and rescue operations, deliver essential supplies to disaster zones, and ensure communication. In cyberspace, cyber intelligence and cyber defense tools are used to identify the sources of attacks, analyze their nature, and neutralize their harmful impact. Swift and coordinated response requires effective cooperation between various government agencies and services, as well as efficient real-time threat information sharing. The use of cyber weapons is a complex issue that requires careful consideration of all potential consequences and compliance with international law [9].

Ukraine continuously faces an increasing number and complexity of cyber threats, which pose a significant danger to national security. State-sponsored cyberattacks–often backed by hostile nations–target critical infrastructure, government institutions, and the private sector with the aims of espionage, sabotage, and destabilization. Cybercrime is also a major concern, involving ransomware attacks, theft of personal data, and financial fraud. These cyber threats can have far-reaching consequences, disrupting essential services, causing significant economic losses, and undermining public trust in state institutions.

As a country on the front line of cyber conflict, particularly in the context of Russian aggression, Ukraine must continuously improve its cybersecurity system and actively engage in international cooperation in this field [6].

Terrorism and extremism remain serious threats to national security in many countries, including Ukraine. International terrorist organizations, as well as domestic extremist groups, may use violence to pursue political, ideological, or religious goals. Terrorist groups actively leverage modern technologies to plan and execute attacks, including using unmanned aerial vehicles (UAVs) for reconnaissance and strikes, as well as encrypted communication channels to coordinate operations and spread propaganda.

Terrorism threats can be both external and internal, often rooted in deep social, economic, and political issues. An effective

counter-terrorism strategy requires a comprehensive approach that includes not only security and law enforcement measures, but also efforts to prevent radicalization, combat extremist ideologies, and address the underlying causes that contribute to the rise of terrorism [6].

Hybrid warfare is a complex phenomenon that combines military and non-military methods to achieve strategic objectives. It includes the use of information warfare, economic pressure, cyberattacks, support for proxy forces, and other unconventional means. Hybrid threats are aimed at undermining a state's internal stability, creating chaos and distrust in authorities, and influencing political processes in favor of the aggressor. Information operations, a key element of hybrid warfare, involve the dissemination of disinformation, propaganda, and manipulation of public opinion to weaken society and erode its will to resist. Countering hybrid warfare requires coordinated efforts from all branches of government, civil society, and international partners to strengthen the country's resilience across all domains [6].

Disinformation campaigns are powerful tools used to influence public opinion and destabilize societies. These campaigns involve spreading false or distorted information to mislead, incite panic, undermine trust in state institutions, and provoke social conflict. In the context of the Russian-Ukrainian conflict, disinformation is one of the aggressor's primary tools aimed at undermining Ukraine's sovereignty and territorial integrity. Social media, online platforms, and emerging technologies – such as artificial intelligence for creating deepfake videos and audio – are actively used to spread such content. Combatting disinformation requires a comprehensive approach that includes enhancing media literacy among the population, supporting independent media, employing technology to detect and debunk fake content, and fostering international cooperation in this field [2; 6].

Artificial intelligence (AI) is a powerful tool in the fight against cyber threats. AI-based systems can analyze vast volumes of network traffic and user behavior data to detect anomalies indicative of cyberattacks. Machine learning algorithms are used to identify malware, phishing emails, and other types of cyber threats. In the context of disinformation, AI can analyze large sets of textual and

visual data to detect fake news, bots, and coordinated disinformation campaigns on social media. AI systems can also automate incident response processes, allowing for rapid threat neutralization and mitigation of consequences. However, it is crucial to remember that malicious actors are also leveraging AI to enhance their attack strategies, making it essential to continually update and advance AI-based defense systems [5; 6].

Unmanned aerial vehicles (UAVs) have become essential tools in counterterrorism operations, enabling surveillance of suspicious individuals and objects, as well as carrying out precision strikes on terrorist targets. Drones are also used to detect and neutralize explosive devices, helping to preserve the lives of security personnel. In border protection, drones are employed to patrol vast areas, detect illegal crossings, and uncover smuggling operations. Satellite imagery and remote sensing data provide valuable information for monitoring borders, identifying military activity, and tracking the movements of terrorist groups. The use of UAVs and satellite technologies allows for real-time intelligence gathering, enhances situational awareness, and reduces risks to personnel during high-risk operations [7].

Cybersecurity technologies play a critical role in defending against hybrid attacks that combine cyber and physical methods of influence. Intrusion detection systems and traffic analysis tools help identify cyberattacks – which are often integral to hybrid operations – at early stages. Encryption technologies and secure communication channels are used to prevent the interception of sensitive information, which is vital in countering information operations, another key component of hybrid warfare. DDoS protection systems help maintain the continuous operation of critical online services and infrastructure, which may be targeted during hybrid conflict. Effective protection against hybrid attacks requires a comprehensive approach that integrates various cybersecurity technologies and fosters coordination among government agencies, the private sector, and international partners [7].

The use of modern technologies in the field of national security is inevitably associated with issues of privacy and personal data protection. Surveillance technologies such as facial recognition

systems, geolocation tracking, and communication analysis are capable of collecting vast amounts of information about citizens, which may lead to violations of their right to privacy. Striking a balance between the need to protect national security and the right to privacy is a complex task that requires clear legal regulation of the collection, storage, and use of personal data in this domain. The absence of adequate legal frameworks can result in abuse and the violation of fundamental human rights [10].

The use of technology in national security may also significantly impact civil liberties and human rights, including freedom of expression and the right to peaceful assembly. Facial recognition systems may be used to monitor participants in peaceful protests, which could have a chilling effect on public demonstrations. It is important to ensure that the application of such technologies does not lead to disproportionate restrictions on these freedoms. Special attention must be given to the bias of artificial intelligence algorithms, which can result in discrimination and unfair outcomes in law enforcement and other areas. To ensure compliance with ethical standards and human rights, it is necessary to develop appropriate ethical guidelines and principles for the use of technology in national security.

The deployment of technologies in the national security sector must also comply with international law, including the laws of war and human rights law. This is especially important in the context of using cyber weapons and autonomous systems, which may have serious consequences for civilian populations and international security. International law has yet to fully adapt to the rapid development of emerging technologies, leading to legal ambiguities and gaps. Therefore, there is a pressing need for international cooperation to establish new norms and principles to govern the use of technology in military and national security contexts, while ensuring respect for fundamental human rights and freedoms [10].

The use of autonomous systems, such as unmanned aerial vehicles and artificial intelligence systems, in the field of national security raises important questions about accountability for their actions. In cases of errors or unforeseen consequences, it can

be difficult to determine who is responsible for the damage caused [2]. The concept of a "human-in-the-loop", which ensures that human oversight is maintained in making critical decisions, is one approach to addressing this issue. Delegating decision-making entirely to autonomous systems may reduce accountability and complicate incident investigations. Therefore, it is essential to develop clear mechanisms of control and responsibility for the use of autonomous systems in national security, ensuring transparency and accountability in their operation [10].

Ukraine actively cooperates with the European Union and the North Atlantic Treaty Organization (NATO) in the field of cybersecurity. Numerous support programs are in place to strengthen Ukraine's cyber resilience, facilitate the sharing of threat intelligence, and conduct joint training exercises. Ukraine participates in collaborative projects to exchange cyber threat data and best practices in cyber defense. Joint exercises and training sessions are held regularly to improve readiness for responding to cyber incidents [10].

Ukraine receives significant financial and technical assistance in cybersecurity from the United States, the United Kingdom, Canada, and other countries. These programs aim to provide Ukraine with essential equipment, software, and expert support to strengthen its cyber defenses. International support plays a crucial role in bolstering Ukraine's cyber defense capabilities, especially amid ongoing aggression.

Ukraine also actively participates in international forums, conferences, and seminars on cybersecurity, where it exchanges knowledge and experience with foreign partners. Joint research projects in the field of cybersecurity and defense technologies are being conducted, enabling Ukraine to access cutting-edge knowledge and innovative developments. Developing international partnerships and engaging in joint initiatives is a key component of strengthening Ukraine's national security [10].

Ukraine cooperates with Western companies and partner countries in the development and implementation of advanced defense technologies, including the production of weapons and military equipment. Ukraine also participates in NATO programs aimed

at the joint development and deployment of cutting-edge military technologies. These joint projects contribute to the modernization of the Ukrainian army and defense industry according to modern standards, while also attracting foreign investment and technology to enhance national defense capabilities.

In the future, the role of artificial intelligence (AI) in the military sphere is expected to grow significantly. Autonomous systems, combat robots, and intelligent command-and-control systems could fundamentally change the nature of warfare [5]. AI may be used for battlefield decision-making, managing large military formations, analyzing intelligence data, and guiding precision weapons. However, the development of AI in military contexts also raises serious ethical and legal concerns, particularly regarding the creation and use of lethal autonomous weapons.

The advancement of quantum computing could introduce new and highly sophisticated cyber threats. Quantum computers have the theoretical ability to break many existing cryptographic algorithms, potentially compromising the security of confidential information, including state and military secrets. This has made the development and implementation of quantum-resistant cryptographic algorithms an increasingly urgent priority [1].

Future developments in biotechnology and its potential use for military purposes are also anticipated. This could include the creation of new types of biological weapons, methods for enhancing soldier performance, and other military applications. Controlling biotechnology development and preventing its use for military purposes has become a critical task for the international community. It is necessary to strengthen international regimes regulating biological weapons and ensure compliance with existing treaties and conventions in this field.

A significant increase in both the volume and quality of disinformation created using AI – particularly deepfake technologies – is expected. Detecting such disinformation will become increasingly difficult, as AI enables the creation of highly realistic fake videos, audio recordings, and texts that are hard to distinguish from genuine content.

Combating AI-generated disinformation will require the development of new verification technologies and methods, along with efforts to boost critical thinking and media literacy among the public [8].

Conclusions. Modern technologies are a powerful tool in ensuring Ukraine's national security, offering opportunities for the detection, prevention, and response to a wide range of threats. However, the rapid advancement of technology also brings new challenges and risks that require constant attention and appropriate countermeasures. To effectively harness technological potential in the field of national security, Ukraine must: Develop and implement a comprehensive national strategy focused on the integration of advanced technologies in the security and defense sector, taking into account the ethical and legal aspects of their use.

Increase public funding for research and development in artificial intelligence, quantum technologies, biotechnology, unmanned systems, and cybersecurity, while encouraging private investment in these areas.

Improve the legislative framework to regulate the use of emerging technologies in national security, ensuring a balance between protecting national interests and safeguarding citizens' rights and freedoms.

Enhance international cooperation with leading countries and international organizations in areas such as information exchange, joint research, and cyber resilience support programs.

Implement educational programs on cyber and media literacy for the general public and government officials to raise awareness of threats and strategies for countering them.

Promote public-private partnerships to stimulate innovation and develop technological solutions tailored to national security needs.

Give special attention to the ethical dimensions of using artificial intelligence and autonomous systems in military and security contexts, ensuring that human oversight remains integral to critical decision-making.

Given the dynamic nature of technological development and the continuous evolution of national security threats, Ukraine must continuously monitor new trends, adapt its strategies, and strengthen

its own technological capabilities to ensure the reliable protection of its national interests in the future.

List of sources used

1. Skitsko O., Skladannyi P., Shyrshov R., Humeniuk M., Vorokhob M. Threats and Risks of Artificial Intelligence Use. Electronic Scholarly Journal Cybersecurity: Education, Science, Technology. 2023. Vol. 2 (22). P. 6–18.

2. Nino Patsuria. Implementation of Artificial Intelligence Technologies in Ensuring Ukraine's National Security and Defense Capabilities: Legal Issues and Post-War Prospects. Theory and Practice of Intellectual Property. 2023. No. 3. P. 68–78.

3. Draft Concept of the State Strategy for the Development of the Bioeconomy of Ukraine until 2030. National University of Life and Environmental Sciences of Ukraine. URL: https://nubip.edu.ua/node/72005 (Last accessed: 15.04.2025).

4. Reznikova O. O. National Resilience in a Changing Security Environment: Monograph. Kyiv: National Institute for Strategic Studies (NISS), 2022. 532 pages.

5. Horobets V. P., Shevchuk O. V., Vasiliev V. V. Application of Artificial Intelligence Technologies in Military Systems: Issues and Prospects. *Information Processing Systems*. 2020. No. 1 (160). P. 133–139. URL: http://lsej.org.ua/6_2023/95.pdf (Last accessed: 15.04.2025).

6. Yakovyuk I. V., Novikov Ye. A., Kupriiova O. O. Modern Technologies and Their Role in Ensuring the Security of the Ukrainian State and Society during Russian Aggression. *Economic Security: International and National Levels:* Proceedings of the 2nd Scientific and Practical Conference, April 21, 2023. Kharkiv: Research Institute of Legal Support for Innovative Development, National Academy of Legal Sciences of Ukraine, 2023. P. 100–107.

7. Lehomynova S., Haidur H. Analysis of Modern Threats to Information Security of Organizations and the Formation of an Information Platform for Countering Them. *Electronic Scholarly Journal Cybersecurity: Education, Science, Technology.* 2023. Vol. 2 (22). P. 54–67.

8. Khaustova V. Ye., Trushkina N. V. Risks and Threats to National Security: Essence and Classification. *Business Inform*. 2024. No. 10. P. 6–22.

9. Khryapynskyi A. P. Spheres of Influence and Tools for Implementing Hybrid Threats: Models and Mechanisms. *State Building*. 2022. No. 2 (32). P. 60–67.

10. Bodnarchuk O. H., Bodnarchuk O. I., Hlukh M. V., Harbinska-Rudenko A. V. Legal Regulation of National Security: Textbook. State Tax University. Irpin, 2024. 202 pages.

ANDROSOV Oleksandr,
PhD candidate (third level of higher education)
in the field of knowledge
05 "Social and Behavioral Sciences" specialty 051 "Economics",
Zaporizhzhia National University,
Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0009-0001-0302-7239

3.2. THE MECHANISM OF CRISIS MANAGEMENT IN THE SPHERE OF NATIONAL SECURITY OF UKRAINE DURING THE RUSSIAN-UKRAINIAN WAR

Introduction. Russia's full-scale invasion of Ukraine in 2022 marked a significant escalation of the conflict that began in 2014, creating a fundamental threat to Ukraine's national security [1]. This has highlighted the urgent need for a reliable and adaptive crisis management mechanism to protect sovereignty, territorial integrity, and national interests [1]. The war exposed vulnerabilities in Ukraine's existing national security system, underscoring the critical need for effective crisis governance. The prolonged and intense nature of the conflict necessitates a shift from reactive crisis response to proactive and adaptive management strategies. The initial stages of the war likely overwhelmed existing protocols, prompting a rapid

evolution in crisis management approaches. Continued aggression demands a system capable not only of responding to present threats but also of anticipating and mitigating future risks.

Effective crisis management is vital for maintaining state functions, protecting citizens, and ensuring the resilience of critical infrastructure during wartime [2]. It involves coordination among various governmental and non-governmental actors to overcome immediate threats and plan for long-term recovery [4]. The ability to manage crises efficiently directly affects Ukraine's capacity to resist aggression and secure its future [1]. The effectiveness of crisis management may prove to be a decisive factor in the outcome of the conflict and the long-term stability of the country. Poor crisis management could lead to systemic failures, erosion of public trust, and an inability to mobilize defense resources effectively. Conversely, a well-functioning system can reinforce national resolve and optimize resource allocation.

Presentation of Key Research Findings. Crisis management involves a system of measures and decisions aimed at diagnosing, preventing, minimizing, and overcoming crisis situations [5]. It is a purposeful activity conducted by national security actors using state capabilities (diplomatic, military, economic, intelligence, and informational) to develop and implement regulatory, coordinating, and monitoring actions. An effective system must be built on principles of anticipation, prevention, and threat mitigation [5]. In the context of national security, crisis management extends beyond economic considerations to encompass all aspects of state security and societal well-being. While some definitions focus on economic stability, the context of war broadens its scope to include military defense, information security, social stability, and the functioning of government institutions under extreme pressure.

The core components of the crisis management mechanism include actors and objects, goals, principles, functions, methods, tools, legal framework, information and communication support, and performance criteria [6]. The key principles are effectiveness, comprehensiveness, coordination, flexibility, and transparency. Crisis management typically proceeds through stages: forecasting, diagnosis, planning,

implementation, control, and evaluation [5]. The multidimensional nature of crisis management requires an integrated approach that encompasses legal, institutional, informational, and strategic elements. Each component is interdependent–for example, successful implementation depends on a solid legal foundation and clearly defined institutional responsibilities, which themselves rely on accurate diagnostics and strategic planning.

Effective crisis management in national security relies on a clear command structure from the President to frontline actors, ministerial accountability for national security agencies, a distinct division between political/strategic leadership and operational command, and the continuous operation and responsiveness of the system regardless of political changes. These principles emphasize the importance of centralized authority, clear accountability, and operational continuity – especially critical in wartime. Any uncertainty in command or responsibility can result in delays and ineffective crisis response. The principle of continuous functioning ensures that the system remains operative even under extreme pressure and political shifts [9].

The Constitution provides a general legal mandate for crisis management in the national security domain, establishing the state's duty to protect its core interests. All subsequent legislation and regulations must align with constitutional principles of national security and the division of powers among branches of government.

The primary legislative acts include the Law of Ukraine "On National Security", which outlines the principles and foundations of security and defense; the Law "On the Legal Regime of Martial Law", which sets the legal basis for martial law including state authority powers and restrictions on rights and freedoms; the Law "On the Defense of Ukraine", which defines the organization and principles of national defense; and the Law "On the National Security and Defense Council (NSDC) of Ukraine", which defines the NSDC's roles and powers. These laws provide concrete legal mechanisms and authorities for implementing crisis response measures within national security and martial law frameworks. The Law on Martial Law is particularly significant as it grants extraordinary

powers to the state during wartime, requiring careful consideration of its implications for civil liberties and democratic governance.

Presidential decrees and Cabinet of Ministers resolutions include orders to impose or extend martial law, enact NSDC decisions, and regulate specific aspects of crisis response and martial law. These acts reflect the practical application of the legal framework, adjusting to evolving security situations and implementing targeted crisis policies. The frequent extensions of martial law underscore the prolonged nature of the crisis and the ongoing need for extraordinary legal measures.

National security strategies and doctrines include the National Security Strategy of Ukraine, which sets priorities, goals, and directions for policy; the Military Security Strategy, which outlines military objectives and approaches; and the Information Security Strategy, which addresses threats and goals in the information domain. These strategic documents define guiding principles for crisis management and outline the state's long-term vision and security priorities. Their development and updates reflect the evolving understanding of national security threats and necessary responses amid the ongoing war [9].

The President of Ukraine serves as the guarantor of state sovereignty, territorial integrity, and national security. The President makes national security and defense decisions through the NSDC and issues decrees on imposing and extending martial law. The President plays a central role in crisis management, holding significant authority in leading national security and defense efforts, especially under martial law. This concentration of power during wartime necessitates robust oversight and accountability mechanisms to prevent potential abuse.

The National Security and Defense Council of Ukraine (NSDC) coordinates and oversees the activities of executive bodies in the areas of national security and defense. It orchestrates efforts to repel armed aggression, protect the population, and maintain public order under martial law. The NSDC plays a key role in strategic planning and decision-making related to national security. As a coordinating authority, it ensures a unified and strategic approach to crisis

management across various government agencies. Its effectiveness depends on facilitating interagency cooperation and ensuring prompt implementation of presidential directives by the relevant executive structures.

The Cabinet of Ministers of Ukraine is responsible for implementing governmental policies on national security and defense. It coordinates and guides the work of ministries and other executive bodies, and develops and approves action plans to implement national security strategies. The Cabinet plays a critical role in translating strategic decisions into specific actions and ensuring seamless government operation during a crisis.

The Ministry of Defense of Ukraine organizes and executes national defense. It commands the Armed Forces of Ukraine, coordinates their responses to military threats, and houses specialized crisis-response units. As the frontline institution in military crisis management, it plays a vital role in defending the country. The ongoing war requires continuous adaptation and enhancement of the Ministry's operational structures, logistics, and coordination with other security branches.

The Security Service of Ukraine (SBU) is tasked with national security, including counterterrorism, counterintelligence, and safeguarding national interests. It monitors and counters non-military threats in information and cyberspace. In the context of hybrid warfare, the SBU is essential in identifying and neutralizing threats beyond the military domain.

The State Border Guard Service of Ukraine secures the country's borders and prevents illicit activities threatening national security. Its role is crucial for maintaining territorial integrity and guarding against infiltration, particularly during wartime, which has escalated its responsibilities and urgency.

Other ministries and agencies – such as the Ministry of Internal Affairs, National Police, State Emergency Service, etc. – also contribute to national security and crisis management. A robust crisis management system depends on the coordinated efforts of these agencies, each with specific duties and expertise. Effective cooperation and information sharing are vital for coherent and timely crisis response.

Rapid mobilization of reserves and territorial defense forces following the full-scale invasion in 2022 exemplified effective crisis management. Military strategy adaptation, logistical adjustments, and supply chain coordination under wartime conditions demonstrated readiness and flexibility, albeit with initial coordination challenges. Analyzing successes and shortcomings from this mobilization offers valuable insights for future crisis management efforts.

Counter-disinformation efforts, morale campaigns, protection of critical information infrastructure from cyberattacks, and strategic communications to inform the public and global partners are prime examples of crisis mechanisms in the information domain. Information security measures have been crucial for maintaining national unity and countering hostile narratives.

Martial law implementation, including its economic impact, regulatory measures, business support mechanisms, and social safeguards, demonstrate economic stabilization efforts. Maintaining economic stability during war requires balancing security needs with economic activity. Evaluating these measures aids in shaping future wartime economic policies.

Humanitarian response, such as evacuating civilians, assisting internally displaced persons (IDPs), and coordinating with international and NGO partners, shows crisis management in humanitarian contexts. The massive population displacement intensified pressure on Ukraine's humanitarian systems and required extensive coordination and resources. Identifying challenges and successes in humanitarian response enhances future crisis readiness.

The NSDC played a pivotal role in coordinating national crisis response across government bodies, issuing critical directives, and shaping wartime strategy. Evaluating the effectiveness of its coordination and decision-making processes is essential for optimizing Ukraine's national security management.

Strategic forecasting and threat assessment to identify potential crises [5], strengthening national resilience across various sectors (economic, social, informational) [4], the development and implementation of national security strategies and doctrines, as well

as international cooperation and partnerships to deter aggression, are essential preventive measures. Proactive actions aimed at preventing crises are crucial for minimizing their impact on national security. Investments in intelligence gathering, early warning systems, and resilience-building initiatives can significantly enhance Ukraine's capacity to withstand future threats [8].

The rapid deployment of forces and resources to eliminate immediate threats, activation of crisis management centers and coordination mechanisms [3], the implementation of martial law measures to ensure public safety and order, and effective communication with the public and stakeholders during crises are key response measures. Swift and coordinated responses are vital for containing crises and mitigating their immediate consequences. Regular crisis response team exercises and trainings, along with clear protocols and communication channels, are essential for effective crisis management.

Military operations to liberate occupied territories and restore territorial integrity, addressing the root causes of the crisis and working toward long-term resolution [7], efforts in post-crisis recovery and reconstruction, as well as reintegration of affected populations and territories, are vital mitigation measures. Overcoming a national security crisis of this magnitude requires continuous and multifaceted efforts encompassing military, political, economic, and social dimensions. The process of overcoming such a crisis is likely to be prolonged and complex, requiring significant resources and international support for recovery and reintegration.

Conclusions. The crisis management mechanism in the field of national security of Ukraine during the Russo-Ukrainian war is a complex and multifaceted system encompassing legislative, institutional, strategic, and practical components. The war has been a severe test for this system, revealing both its strengths – such as the ability for rapid mobilization and adaptation – and its challenges related to coordination, efficiency, and long-term resilience. International cooperation and assistance have played a crucial role in supporting Ukraine in its struggle against the aggressor.

To further strengthen the crisis management mechanism in Ukraine's national security domain, it is recommended to:

– Enhance interagency coordination and information sharing among all actors involved in national security and crisis management.

– Continue developing strategic forecasting and early warning systems for better anticipation of potential crises.

– Pursue adaptation and modernization of the legal and regulatory framework for crisis management based on the lessons of the ongoing war.

– Invest in training and capacity-building for personnel involved in crisis management at all levels.

– Strengthen the national resilience of critical infrastructure and essential services to minimize vulnerability to future threats.

– Develop a comprehensive long-term strategy for post-war recovery and reintegration with clearly defined roles and responsibilities for all stakeholders.

– Continue strengthening international cooperation and partnerships across all areas of national security and crisis response.

– Raise public awareness and media literacy to counter disinformation and enhance societal resilience.

– Implement robust monitoring and evaluation mechanisms to assess the effectiveness of crisis management measures.

List of sources used

1. Ponomarenko O., Morozyuk Y., Ninyuk M. The Impact of Military Actions on the Effectiveness of Public Administration in Ukraine. *Akademichni Viziï (Academic Visions).* 2024. Issue 32. URL: https://academy-vision.org/index.php/av/article/view/1198/1069 (Last accessed: 15.04.2025).

2. Chechotka V. D. Features of Public Administration Functioning in Ukraine under Wartime Conditions. *Scientific Notes of the V. I. Vernadsky Taurida National University. Series: Public Administration and Management*. 2023. No. 5, Vol. 34 (73). P. 7–12. URL: https://periodicals.karazin.ua/db/article/download/22952/20996/ (Last accessed: 15.04.2025).

3. Education and Science in the Field of National Security: Problems and Development Priorities: Proceedings of the 6th International Scientific and Practical Conference (Ostroh, May 17, 2024) / Edited by M. S. Romanov, R. S. Martynyuk, E. M. Balashov. Ostroh: Publishing House of the National University "Ostroh Academy", 2024. 319 p. URL: https://cutt.ly/irgrtlGO (Last accessed: 15.04.2025).

4. On the Coordination of Activities for Building National Resilience (Strategic Level). Analytical Note. Series "National Security". URL: https://niss.gov.ua/sites/default/files/2020-02/analit-resnikova-national-security-9-2020-1.pdf (Last accessed: 15.04.2025).

5. Sak T. V., Yushchyshyna L. O. The Mechanism of Crisis Management in the Context of Ensuring Economic Security of an Enterprise. *Economic Journal of Lesya Ukrainka Eastern European National University.* 2019. Vol. 2, No. 18. P. 66–74. URL: https://surl.li/guvyob (Last accessed: 15.04.2025).

6. Oleshko A. A. The Mechanism of Crisis Management of Financial Corporations. *Effective Economy*. 2018. No. 2. URL: http://www.economy.nayka.com.ua/pdf/2_2018/12.pdf (Last accessed: 15.04.2025).

7. Myskyv V., Bilyk V. Stages and Measures of Crisis Management at the Enterprise. *Management and Entrepreneurship in Ukraine: Stages of Formation and Development Issues.* 2024. Vol. 6, No. 1. P. 25–31. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/sep/35776/240560maketmanagement-23-31.pdf (Last accessed: 15.04.2025).

8. Pohrebniak A. Yu. The Essence of the Components of the Crisis Management Mechanism at an Industrial Enterprise. *Economic Bulletin of NTUU "KPI"*. 2015. No. 12. P. 138–147. URL: https://ev.fmm.kpi.ua/article/view/45627 (Last accessed: 15.04.2025).

9. Lyashevska O. I. Improvement of the State Crisis Management Mechanism in Ukraine under Martial Law Conditions. *Bulletin of the National University of Civil Protection of Ukraine. Series: Public Administration.* 2024. 1 (20). P. 159–165. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/20346/1/19Liashevska.pdf (Last accessed: 15.04.2025).

GORBUNOVA Anna,
Ph.D. in Economic. Sc., docent,
Zaporizhzhya National University,
Ukraine, Zaporizhzhya
ORCID: https://orcid.org/0000-0001-6450-4740

KAIRACHKA Nataliia,
master's student,
Zaporizhzhya National University,
Ukraine, Zaporizhzhya
ORCID: https://orcid.org/0009-0001-4537-217X

3.3. DIGITALIZATION AS ONE OF THE METHODS OF FORMING THE COMPETITIVENESS, ADAPTABILITY AND FLEXIBILITY OF A CORPORATION DURING THE POST-WAR RECONSTRUCTION OF UKRAINE

Introduction. Despite the hostilities, as well as other difficulties arising from current events, in 2024 Ukraine received the fifth place in the field of development of electronic public services, as well as the first place in the E-Participation index. The expansion of areas and industries of digital services is important for ensuring effective transformational digitalization processes. The volume of planned expenditures for digital reconstruction and development by 2025 occupies the largest share of expenditures for the development of the digital economy (49.6 %), 25.5 % of the total expenditures are planned for the reconstruction of the digital network of ASCs, amounting to 11.87 %. Let's note the fact that in 2022, Ukraine joined the Digital Europe program until 2027. All these developments provide the basis for expanding digitalization processes at domestic enterprises, ensuring high competitiveness, adaptability and flexibility of the corporation for the post-war reconstruction of the domestic infrastructure to ensure future economic prosperity.

Presentation of the main results of the research. In the hour of uncertainty, the financial crisis, which was caused by the outbreak

of military operations, as well as the global economic disruptions in the international arena, has an ongoing nature, which creates a culprit of factors that pose a threat, manifested by increased competitiveness among current foreign technological enterprises. Therefore, given the current situation, there is an increasing need to adapt to internal and external factors that help increase the level of adaptation of Ukrainian IT companies. It should be noted that over the past 12 years, including until 2022, stagnation was observed in the IT industry. Growth on average ranged from 25–30 %. It can be stated that after 2022, the situation in this market deteriorated due to the war, which affected the increase in the volume of non-fulfillment of contract orders. In 2024, the total export revenue of IT services decreased and amounted to $5.8 billion in 11 months. Thus, in order for the situation to change for the better in 2025, it is necessary to solve the main problems in this area: mobilization and difficulties with obtaining a deferment for key specialists; difficult situation in some IT clusters, primarily in Kharkiv; limited opportunities to travel abroad; missile attacks and related blackouts; increased tax burden.

This will help to adapt to the current conditions of uncertainty, overcoming the existing negative aspects inherent in IT spheres. Therefore, digitalization is becoming more relevant, as it is one of the most important directions of growth of human civilization, which allows us to focus on determining the main directions of improving the management mechanisms of technology companies. Expanding access to healthcare, education, and banking will come through the creation of an inclusive society. This will help improve the quality and coverage of public services, expand the way we interact with customers, and expand the range of goods and services at lower prices.

As of the current period, digital technologies are part of business processes in IT companies, which is manifested in the export reduction of the cost of cloud technologies, the cheapening of the cost of software development itself, the increase in free content and services, and the creation of unique products adapted to the client's preferences [7].

Currently, the Ukrainian authorities are engaged in the spread of digitalization processes within the country, including the following

main trends in the transformation of technological enterprises: blockchain, the Internet of Things, cloud computing and digital security, information gathering from various sources, and the impact of 5G. The essence and significance of these technologies are presented in Fig. 1.

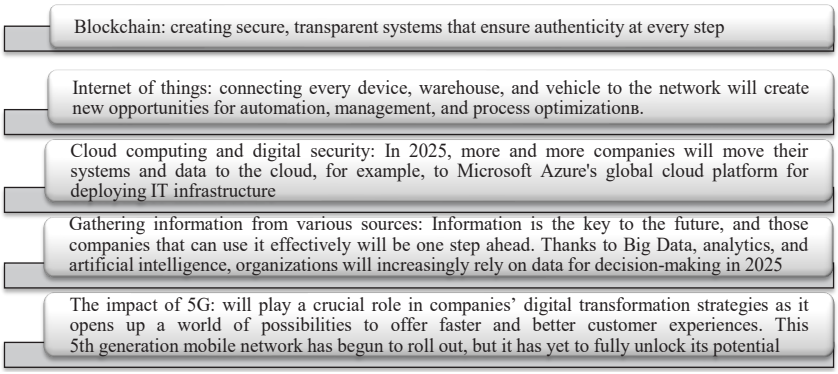

Fig. 1. Key trends in the digitalization of technological enterprises in Ukraine as of 2025

Source: [8; 9]

As a foreign experience of the main digital trends, Finland was taken and the Finnish company Nokia was considered. This Finnish multinational corporation was founded on May 12, 1865 as a single paper factory. Nokia. In 2014, Nokia's mobile phone business was sold to Microsoft [5].

We examined three projects of the Finnish company Nokia: "6G-ANNA", "LEAD leading company" and "SUSTAIN-6G". Nokia is the overall leader of "6G-ANNA", a 6G beacon project funded by Germany. The "6G-ANNA" project is making a significant contribution to the development of technologies that enable the implementation of 6G. The German economy can accumulate the necessary know-how to later independently use 6G networks. Incentives are also being created to increase the production of key components in Germany and Europe. At the same time, it will be ensured that the requirements of leading German industries are included in the 6G standard. In this way, 6G

technologies will become part of the cutting-edge technologies in leading industries at an early stage. Overall, the project results make a significant contribution to the technological sovereignty of Germany and Europe [12]. Fig. 2 shows the storyline of the "6G-ANNA" project, the concept for the German 6G beacon project.

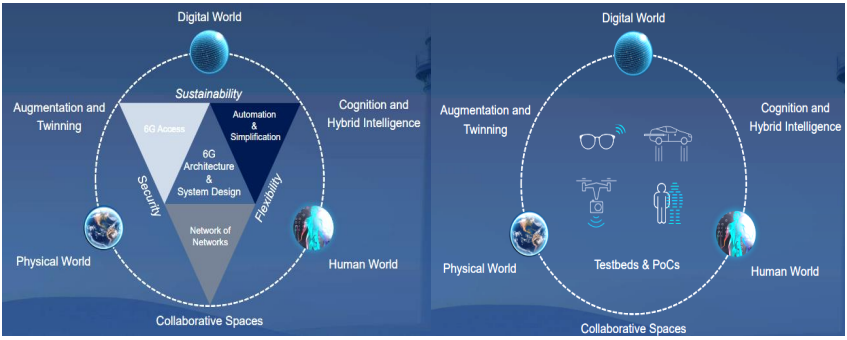

Fig. 2. Concept for the German project "Mayaka 6G": the storyline of the project "6G-ANNA"

Source: [13, p. 5–6]

In 2023, the Finnish company Nokia participated in the competition of leading companies 2023, the other winners of which were Kempower, Patria, Valio and Wärtsilä. The project of the Finnish company Nokia was aimed at developing increased usability, security and energy efficiency of the future internet and metaverse. Therefore, in view of the victory, the Finnish government organization for financing innovation, trade, travel and investment promotion, Business Finland, allocated funding for the Nokia "LEAD leading company" project, the goal of which is to increase the usability, security and energy efficiency of the future Internet and metaverse [10].

It is worth noting that the industrial metaverse is a growing market and offers great business opportunities for Finnish companies. The metaverse refers to a solution that seamlessly connects the physical and digital worlds. For example, the metaverse allows for real-time collaboration, simulation, and remote work.

There are three types of metaverses: consumer metaverse, industrial metaverse, and corporate metaverse. These three types of metaverses, although serving different purposes, will have common features in the future. Different types of metauniverses will be interconnected to varying degrees, and will share common technologies, devices, and interfaces. It is anticipated that each instance of the metauniverse will serve different companies, communities, and users.

Note that the consumer metaverse is primarily focused on entertainment and leisure, while the corporate and industrial metaverses are focused on business applications [6].

Thanks to this flagship corporate project, Nokia has significantly increased its own and partner investments in research, development and innovation (RDI) in Finland.

Already in 2024, the Finnish company Nokia was selected by the Smart Networks and Services Joint Venture (SNS JU) as the leader of the "SUSTAIN-6G" project. This project is designed for 2027 and includes the following industry areas:

– smart power systems: development of microgrids with real-time control based on artificial intelligence for efficient and redundant electricity distribution;

– e-health and telemedicine: Expansion of 6G infrastructure for secure exchange of medical data and remote diagnostics, improving healthcare in underserved areas;

– agriculture: Using 6G technology for agricultural applications with high bandwidth, data analysis and automation, increasing productivity and sustainability [11].

So, let's summarize that the SUSTAIN-6G project is one of the flagship projects of the SNS JU. It significantly strengthens Nokia's leadership in the field of innovative developments. This initiative, together with the Hexa-X and Hexa-X-II projects, helped the Finnish company Nokia lay the foundation for the preliminary standardization of 6G and studied possible options for its use. In addition, the consortium includes various stakeholders, including network equipment suppliers, telecommunications operators, research institutes, industrial manufacturers and SMEs, which provide a comprehensive approach to the development of sustainable innovations.

If we consider the sphere of leadership of the Finnish company Nokia, then Table 1 indicates that it covers organizations for standardization of mobile communication networks, formation of the 5G and 6G ecosystem, organizations for standardization of fixed access, organizations for IP routing, Ethernet switching and optics standardization, and multimedia organizations.

Table 1

Leadership of Finnish company Nokia in the field of intellectual property rights

The name of the field of leadership	The main characteristic
1	2
Mobile network standardization organizations	Including 3GPP and the seven joint standards development organizations ETSI, ATIS, ARIB, TTC, TTA, CCSA and TSDSI. Nokia is also active in industry organizations that promote mobile network technologies and standards, including O-RAN Alliance, GSMA, GSA, 5G Americas and NGMN.
Shaping the 5G and 6G ecosystem	In 2016, Nokia founded the 5G Automotive Association (5GAA). In 2018, Nokia created the 5G Alliance for Connected Industries and Automation (5G-ACIA). And in 2024, Nokia became a founding member of the AI-RAN Alliance. Today, Nokia is shaping the 6G ecosystem and is actively involved in, among others, the NextG Alliance in the US, SNS 6G-IA in Europe and Bharat 6G Alliance in India.
Fixed access standardization organizations	Nokia plays a leading role in standards organizations such as the Broadband Forum and IEEE 802.11. Our active participation in these groups ensures the development of reliable and interoperable fixed access technologies. In addition, we collaborate with key regional standards organizations to support and advance the advancements in local area networking. Nokia was one of the six founding members of the Wi-Fi Alliance in 1999.

Continuation of Table 1

1	2
IP routing, Ethernet switching, and optics standardization organizations	Nokia actively participates in IP routing, Ethernet switching, and optical standardization organizations, including IETF, IEEE 802, ITU, OIF, and ONF. Our participation helps ensure the advancement and interoperability of global networking technologies.
Multimedia organizations	Nokia is an active participant in the Metaverse and MPEG Standards Forum. Our participation helps shape the future of video and audio standards and technologies.

It can be said that digitalization processes help to ensure effective anti-crisis management, which is an interconnected comprehensive company management system characterized by a strategic focus, created to identify and eliminate current and future problems in operations by developing and implementing an effective and modern program of anti-crisis measures [1]. Its main identifiers in terms of forming a company's reputation are competitiveness, adaptability, and flexibility.

Competitiveness in business refers to a company's ability to balance the price and quality of its products and services to provide customers with an optimal experience. Furthermore, competitiveness in business refers to a company's ability to achieve greater sales or customer loyalty than its competitors, due to the quality of its products and services, low prices, or a combination of both factors [2].

Competitiveness in business can be divided into two areas: price competitiveness, when a business can maintain the quality of its goods or services while keeping prices lower than those of its competitors, and structural competitiveness, when a business can maintain better sales or customer loyalty compared to its competitors regardless of the prices it offers.

Note that the concept of "adaptability" is defined as "the ability of a person to adapt to changes in the environment. When you think about your career aspirations, changes directly affect how flexible you can be. The practice of adaptation can include how quickly you are able to respond to change".

Change is a natural part of life; therefore, the ability to adapt is a crucial skill. Active participation helps to embrace change, understand it, be receptive, open, and adaptable.

The third dimension of crisis management in terms of company reputation is flexibility. Workplace flexibility is a strategy for responding to changing circumstances and expectations. Employees who approach their work with a flexible mindset tend to be more valued by employers. Similarly, employers who cultivate a flexible work environment are attractive to employees [4].

A flexible workplace meets the needs of both the employee and the employer. Workplace flexibility is often used as a tool to retain and engage employees. It can also help an organization achieve its goals by increasing productivity. It can be said that the main objects of the mechanism of functioning of work flexibility are employees, employers and the schedule.

As one of the reputational anti-crisis measures to increase competitiveness, adaptability and flexibility, this multinational company applies its code of conduct, which identifies specific risks and problems that employees of international companies may face. Its main points are listed as Nokia's compliance policy in table 2.

In addition, Nokia's corporate governance practices, which comply with Finnish laws and regulations, Nokia's articles of association, the finnish corporate governance code 2020 and the corporate governance standards of the following stock exchanges, were considered as a second anti-crisis management measure: Nasdaq in Helsinki, Euronext in Paris and the New York Stock Exchange ("NYSE").

To briefly describe the essence of the Corporate Governance Code, we note that it is a collection of recommendations on good corporate governance for companies listed on the stock exchange. The recommendations of the corporate governance code supplement the obligations set out in the legislation. the purpose of the corporate governance code is to maintain and promote high quality and international comparability of corporate governance practices applied by Finnish listed companies.

Table 2

Code of conduct: Nokia compliance policy

Name	Essence
1	2
Conflict of interest	The company's activities are carried out in the interests of Nokia and use information, property, resources primarily for the benefit of Nokia and to support Nokia's business needs.
Communication with government officials	Nokia engages with international organizations, governments, officials and policymakers at various levels and in various ways, including as a company providing products and services.
Fair competition	Nokia competes fiercely but fairly. Competition laws (or antitrust laws) regulate the activities of companies, ensuring fair competition in the interests of consumers and other market participants.
Improper payment	Nokia conducts its business and deserves what it deserves. The corporation will not tolerate improper or corrupt payments, including bribes or kickbacks, made directly or indirectly to a customer, government official or third party, including improper gifts; entertainment, gratuities, donations for services such as favorable contract terms, job selection or ignoring normal procedures.
Compliance with trade standards	Nokia is committed to complying with all applicable trade laws and regulations that affect its operations, including export controls, sanctions, anti-boycott and customs compliance. The Corporation is committed to preparing, conducting and reporting international business transactions to trade authorities accurately and transparently.
Working with third parties	Nokia is committed to productive, ethical and transparent relationships with its third parties. The corporation expects all third parties to meet Nokia's standards, comply with and exceed all applicable laws and regulations, and share its values.
Environment	Nokia is constantly striving to prevent environmental pollution and reduce the environmental impact of its products and services during design, procurement, production, use and end-of-life.

Continuation of Table 2

1	2
Fair employment	Management respects all people, regardless of their personal characteristics protected by law. These include age, disability, gender identity, gender characteristics or expression, race, religion or belief, sex, and sexual orientation.
Occupational health and safety, safety techniques and working conditions	The corporation deserves the respect of each other, its contractors, partners, customers and members of the public by providing a safe, healthy and fair work environment.
Human rights	Nokia adheres to the principles of the Universal Declaration of Human Rights and the United Nations General Declaration of the Guiding Principles on Business and Human Rights, and expects its suppliers and business partners to share these values.
Privacy and data protection	Nokia's Privacy Policy embodies the principles of privacy. We design our products and services with privacy and security in mind, and we take all available safeguards to protect your personal data from unauthorized use or disclosure, while maintaining its confidentiality.
Management	Nokia is committed to complying with applicable laws and regulations in all countries where Nokia operates, which govern its financial accounting and reporting to government agencies, investors and the public.
Intellectual property and confidential information	Nokia's intellectual property, which includes patents, software and other copyrighted material, know-how and trade secrets, as well as brands and trademarks, is one of the company's most valuable assets.
Insider trading	In the course of their work, employees may become aware of material, non-public information about Nokia or other companies. Using this material, non-public information for personal or financial purposes, such as buying or selling shares, or disclosing this information to others, undermines market integrity, violates corporate policy, and may be a violation of the law.

Source: [6]

Effective corporate governance contributes to the value creation of Finnish listed companies and their attractiveness as investment objects.

So, let us highlight that in the current situation, one of the natural, most effective and fastest directions for the further development of Nokia Corporation is not only increasing the degree of adaptation and flexibility of enterprises to market needs, but also increasing their competitiveness. To this end, the corporation must use all available opportunities to ensure the widespread use of advanced techniques and progressive technologies already available and used worldwide, the implementation of which will contribute to further effective compliance with the Code of Conduct and the organization of effective corporate governance on the stock exchange in accordance with Finnish laws and regulations.

Conclusions. Based on the analysis, we see that the IT sector provides development prospects and competitive advantages for both SMEs and large companies. However, in Ukraine there are aspects in this area that need to be improved. Thus, only half of medium-sized enterprises (48 %) have a website, and only a third (30 %) of small enterprises. Regarding social media, the use of this communication tool is approaching the frequency of website use. The tool is used by 52 % of large companies and only about 36 % and 27 % of medium and small enterprises, respectively. Some enterprises demonstrate limited use of digital tools.

Therefore, the implementation of developments of foreign corporations and the improvement of financial literacy among employees of technological enterprises in Ukraine, strengthening and improving the level of competitiveness, adaptability and flexibility of domestic enterprises during the post-war reconstruction of Ukraine, are becoming increasingly important today.

List of sources used

1. Stroiko Tetiana, Kharus Hanna. Anti-crisis management as the basis of ensuring the economic stability of enterprises. *Three Seas Economic Journal.* 2022. Vol. 3 No. 4. P. 44–51. URL: https://www.researchgate.net/publication/368412743_ANTI-CRISIS_MANAGEMENT_AS_THE_BASIS_OF_ENSURING_THE_ECONOMIC_STABILITY_OF_ENTERPRISES (Last accessed: 14.02.2025).

2. Indeed for employers. How Can You Define Competitiveness in Business? URL: https://www.indeed.com/hire/c/info/competitiveness-definition#:~:text=Competitiveness%20in%20business%20refers%20to,customers%20with%20the%20optimal%20experience (Last accessed: 15.02.2025).

3. It's your Yale. Learn and Grow: What is adaptability in the workplace? URL: https://your.yale.edu/learn-and-grow-what-adaptability-workplace#:~:text=New%20managers%20and%20employees%20are,to%20changes%20in%20their%20environment (Last accessed: 16.02.2025).

4. The balance. What Is Workplace Flexibility? URL: https://www.thebalancemoney.com/workplace-flexibility-definition-with-examples-2059699#:~:text=Workplace%20flexibility%20emphasizes%20the%20willingness,for%20retaining%20and%20engaging%20employees (Last accessed: 17.02.2025).

5. wikiwand. URL: https://www.wikiwand.com/en/articles/History_of_Nokia (Last accessed: 18.02.2025).

6. NOKIA. URL: https://www.nokia.com/about-us/ (Last accessed: 19.02.2025).

7. Razumkov Center. Digitalization: Benefits and Ways to Overcome Challenges. URL: https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv (Last accessed: 20.02.2025).

8. Digital business transformation: 5 trends for 2025. URL: https://hub.kyivstar.ua/articles/czifrova-transformacziya-biznesu-5-tendenczij-2025-roku (Last accessed: 21.02.2025).

9. Digital transformation: what to expect in 2025 and beyond. URL: https://fueled.com/blog/digital-transformation-predictions-2025/ (Last accessed: 22.02.2025).

10. Arctictoday. Nokia is developing applications for the industrial metaverse with Business Finland's leading company funding. URL: https://www.arctictoday.com/%F0%9F%87%AB%F0%9F%87%AE-nokia-is-developing-applications-for-the-industrial-metaverse-with-business-finlands-leading-company-funding/ (Last accessed: 23.02.2025).

11. Nokiamob. Nokia Leads Major European Project on Sustainable 6G Development. URL: https://nokiamob.net/2024/10/30/nokia-leads-major-european-project-on-sustainable-6g-development/ (Last accessed: 23.02.2025).

12. Bundesministerium für Bildung und Forschung. Projekte. 6G-ANNA. URL: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/6g-anna (Last accessed: 24.02.2025).

13. Dr. Marco Hoffmann, Dr. Rastin Pries Nokia. 6G-ANNA. Concept for a German 6G Lighthouse Project. Seite 2–7. URL: https://d1p0gxnqcu0lvz.cloudfront.net/documents/6G_ANNA_presentation.pdf (Last accessed: 24.02.2025).

MORDVINOVA Iryna,
Lecturer in Economics,
Senior Lecturer of the Separate structural subdivision
"Economics and Law Specialist College
of Zaporizhzhia National University",
Zaporizhzhia, Ukraine

3.4. FEATURES OF THE USE OF DIGITAL TECHNOLOGIES IN THE SERVICE SECTOR: SCIENTIFIC AND PRACTICAL ASPECT

Introduction. Today, modern business is increasingly moving into the digital environment, and service companies are forced to adapt to new conditions to remain competitive. Customers expect fast, convenient and personalised services that are made possible by digital tools. Digital technologies help automate routine operations, reduce costs, improve logistics and human resources management. In addition, the impact of COVID-19 has accelerated the introduction of contactless services, online services and remote communication channels, which has become the new normal. The use of artificial intelligence, Big Data, CRM systems, and the Internet of Things

(IoT) is helping to create new approaches to customer service. Digital technologies allow small companies to compete globally using online platforms, marketplaces and social networks. Therefore, research in this area helps to understand how to effectively integrate new technologies into business service models, provide a better customer experience and stimulate business development.

Presentation of the main results of the study. Today, many scientists are actively studying the peculiarities of using digital technologies in various fields of activity, as this is one of the key topics of modern science and practice. For example, K. Kraus, N. Kraus and O. Marchenko [1] focused on the study of the peculiarities of using the digital technology of the Internet of Things and the latest CRM systems. The authors noted that the digital transformation of modern business changes the forms of activity, restructures organisations, opens up new sources and forms of income, allows attracting more consumers and bringing customer service to a qualitatively new level. The article [2] investigates the peculiarities of using digital technologies in business activities, due to their crucial importance in ensuring the market competitiveness of business entities. Digital tools significantly transform business models, operational processes, channels of communication with consumers, and management approaches. The article also focuses on key areas of their application: e-commerce, digital marketing, financial technologies and customer relationship management (CRM) systems. I. Borysov in his study 'analysed the current legislation in order to identify the impact of the development of information technology on ensuring proper legal regulation of relations in the field of service provision in the context of digitalisation' [3]. T. Zabashtanska, I. Shpirnov and M. Mykhailiuk 'studied the types of digital technologies used in the financial services market of Ukraine, noted the advantages and disadvantages of introducing and using modern digital technologies by financial services market participants' [4]. Among the disadvantages of the practical implementation of the introduction of digital technologies, they noted the low level of financial and digital literacy of consumers of digital financial services, while the advantages are quick access

to banking, insurance, and investment services, cost reduction, personalisation of communications, etc. The authors of article [5] studied the role of digital technologies in transforming business models of modern enterprises, compared traditional and new (digital) business models, and identified the benefits of digital transformation for modern enterprises. As a result, they concluded that digital business models (the latest ones) allow enterprises to be more flexible, efficient and competitive, which is necessary in today's rapidly changing digital environment. U. Balyk, I. Losheniuk, and T. Vader [6] noted that one of the strategic directions of international marketing activities of modern companies is the use of digital technologies as an effective tool for conducting economic activity. In a globalized market environment, digital solutions provide businesses with the opportunity not only to optimize marketing processes, but also to establish direct contact with target audiences in different geographic markets. As part of international marketing, digital tools significantly reduce communication costs, accelerate entry into new markets, increase the accuracy of market risk assessment, and contribute to effective brand positioning. In the study, Y. Stashenko and O. Gavrylovsky [7] considered the concept and essence of digital transformation in trade as one of the key areas of development of the modern economy. Digital transformation in the field of trade not only simplifies and automates business processes but also creates fundamentally new opportunities for companies to grow, scale and enter international markets. Thanks to digital tools, enterprises gain access to new sales channels, expand their target audience, improve the quality of customer service and increase operational efficiency. But the study of the use of digital technologies in the service sector as a key factor in the modernization of service activities, which contributes to increasing the efficiency of business processes, improving customer experience and ensuring the competitive advantages of enterprises, namely: the introduction of digital platforms for online service; the use of mobile applications, digital customer relationship management (CRM) tools; automation of service processes and personalization of services, etc.

The service sector is a set of branches of the national economy that do not create tangible goods but produce a special type of product – a service, which is the result of purposeful, justified activity aimed at satisfying certain needs of the consumer. Services can be both tangible (repairs, transport) and intangible (education, finance, medicine, consulting), and, unlike goods, do not have a physical form and, as a rule, are consumed at the time of provision. In modern conditions of digitalization, this area demonstrates the highest dynamics of development due to the widespread introduction of innovative technologies.

The service sector is one of the three sectors of the economy, which contains all types of commercial services. We are talking about financial, hotel and restaurant, tourist, transport, retail, insurance, medicine, education, entertainment, marketing, etc. Service in the service sector is focused on meeting the needs and desires of customers and solving their problems [8].

In countries with high rates of technological development, the service sector plays a leading role in the economy, providing up to 70 % of the gross domestic product (GDP). At the same time, the level of employment in the service sector is more than 50 % of the total number of the working population [8].

The service sector is gradually gaining a leading position in the economy, ahead of traditional commodity production in terms of development. It demonstrates high dynamism, flexibility and the ability to quickly adapt to changes in market conditions and growing consumer expectations.

The service sector has its own characteristics:

– combination of production and sales in one product;

– absolute dependence on the demand for a particular service and its specifics, including seasonality;

– the presence of large and small organizations in the market;

– priority of psychological, professional, social training of employees;

– the possibility of serious territorial separation of different divisions of organizations [9].

So, the main feature of this area is its focus on the individual needs of the client, which forms new approaches to business organization, marketing and communications. The main digital technologies that are actively used in the service sector (especially in tourism, hotel and restaurant business, retail, finance, etc.) are presented in Table 1.

The importance of key digital technologies in the service sector lies in the fact that they fundamentally change the approach to service delivery, making it faster, more convenient, personalised and scalable.

Table 1

Basic digital technologies in the service sector

Technology	Contents	Effect
1	2	3
Artificial intelligence (AI) and machine learning	Chatbots and virtual assistants (for example, in 24/7 customer support). Personalisation of offers, analysis of customer behaviour. Demand forecasting and marketing automation.	Improving the quality of customer service. Personalisation of services. Automation of routine processes. Forecasting demand and customer behaviour. Reducing costs. Improving marketing. Risk and security management.
Cloud computing	Online services for booking, data storage, and personnel management. Flexible access to systems from any device and reduced IT infrastructure costs.	Accessibility of information at any time and from any place. Reducing the cost of IT infrastructure. Fast scaling. Improved data security. Facilitate collaboration between departments and branches. Integration with other services
Mobile applications	Online booking, food ordering, reviews and payment. A convenient channel of interaction with consumers in real time.	Convenience for customers. Increased loyalty. Quick feedback. Optimisation of service processes. Increase in sales. Contactless service.
Big Data	Analysing large amounts of information about customers, sales, and market trends. Creating targeted offers and business development forecasts.	Deep understanding of customers. Demand forecasting. Optimisation of marketing. Improving the quality of service. Formation of pricing policy. Reducing costs.

Continuation of Table 1

1	2	3
Internet of things (IoT)	"Smart hotel rooms: climate, light, and smartphone access control. Connecting equipment to a single system for easy management.	Improving the customer experience. Automation of processes. Saving resources. Improved security. Quick response to malfunctions. Personalised service.
Augmented and virtual reality (AR/VR)	Virtual tours of hotels or tourist attractions. AR menus in restaurants, interactive experience for customers.	Virtual tours before buying. AR menus in restaurants. Improved customer interaction. Effective staff training. Personalisation of the tourist experience. Attracting a young audience.
E-commerce and online platforms	Integration with booking, delivery, and e-commerce websites. Electronic payment systems (PayPal, Apple Pay, Google Pay).	Availability 24/7. Expansion of the market. Convenience of payment. Increase in income. Automation of processes. Systematisation of reviews and ratings. Effective marketing.
CRM-systems (Customer Relationship Management)	Automated customer relationship management. Keeping a history of orders, contacts, individual offers.	Centralised storage of customer information. Personalised service. Automation of interaction. Analytics and reporting. Improving the level of service. Sales and repeat order management.
Automation systems	POS systems in restaurants and hotels. Software for booking, warehouse, and personnel management.	Speed up customer service. Reducing errors. Full analytics of business processes. Cost optimisation. Improving the quality of service. Improved staff control. Integration with other systems.

Source: compiled by the author

The use of artificial intelligence (AI) in the service sector has a tangible effect on both businesses and consumers. Cloud computing

allows businesses to be flexible, scalable and efficient. The use of mobile applications in the service sector has a significant beneficial effect, as they create convenience for customers and increase business efficiency. Big Data allows businesses to better understand customers, make informed decisions and increase profitability. The use of the Internet of Things (IoT) in the service sector brings tangible benefits, as it makes services smarter, faster and more convenient for both customers and businesses. The use of augmented reality (AR) and virtual reality (VR) creates an immersive, interactive and personalised experience that offers many practical benefits for businesses and customers. The use of e-commerce and online platforms significantly expands access to services, simplifies customer interaction and opens up new revenue channels. CRM (Customer Relationship Management) systems in the service sector help businesses understand their customers better, automate interaction with them and improve the quality of service. The automation system allows you to increase the speed, accuracy and quality of service, reducing costs and the human factor. Thanks to digital tools, businesses can improve customer experience, reduce costs, increase service quality, and compete effectively in the marketplace.

Globally, the tourism and hotel and restaurant business is one of the key components of the service sector, which plays an important role in shaping the national economy, creating jobs and generating budget revenues. For example, in 2024, the tourism sector of Ukraine brought almost UAH 3 billion to the country's budget, which is 89 % more than in 2021 [10]. These industries provide a wide range of services – from organising travel and excursions to accommodation, food and leisure for tourists.

The travel and hospitality industry is one of the most competitive segments of the service sector. This is due to the high market saturation, constant changes in consumer preferences, seasonality of demand, and the availability of a wide range of offers for customers in both physical and digital environments. Digital technologies are becoming an important tool for increasing competitiveness, allowing to optimise business processes, personalise services, interact

effectively with customers and respond quickly to changes in the market situation.

In global practice, digital technologies have become an integral part of the development of the tourism and hotel and restaurant business. Global companies and local businesses are actively implementing innovative solutions to increase efficiency, improve service quality, personalise services and create competitive advantages. For example, Disneyland in the United States is one of the most prominent examples of how artificial intelligence (AI) and augmented reality (AR) are used to improve customer experience and increase park attendance. The company is actively integrating these technologies to make the visit experience even more immersive, personalised and convenient for guests [11]. China is actively using facial recognition at airports, hotels, and tourist attractions. Passengers can go through security without having to show passports or tickets. This significantly reduces the time required for check-in and customs clearance [12]. For China, this is part of the country's strategy to develop safety, convenience and innovative solutions in everyday life. The experience of the African tourism region, a continent with rich natural potential, is among the practices of using digital technologies in the tourism business. Kenya and Tanzania are among the leaders in the implementation of eco-friendly technologies in the tourism sector, particularly in the field of safaris and tourism in national parks. Both countries are actively developing mobile platforms for booking tours and using modern technologies to preserve ecosystems, support sustainable development and provide convenience for tourists [13]. Thus, the use of digital technologies in the tourism and hospitality industries develops differently depending on the region: Europe is focused on sustainability and mass digitalisation, the US relies on tech start-ups and personalisation, Asia is actively implementing AI and smart technologies, and Africa and Latin America are focusing on ecotourism and mobile solutions.

Digital technologies in the travel and hospitality industry are opening up many new opportunities to improve service, increase efficiency and customer convenience.

Fig. 1 shows the main advantages of using digital technologies for the tourism and hotel and restaurant business as a service industry.

Facilitating the booking process	Personalisation of services	Improving customer service	Mobile payments and contactless payments	Collecting and analysing customer feedback
– mobile applications and web platforms; – interactive online platforms (Booking.com, Airbnb, OpenTable)	– data analysis; – use of CRM systems	– chatbots and artificial intelligence (AI); – AI-based digital assistants	– contactless payments via smartphones (Apple Pay or Google Pay); – QR-codes	– big data analysis; – digital platforms (TripAdvisor, Yelp)

Fig. 1. Main advantages of using digital technologies for the tourism and hotel and restaurant business

Source: compiled by the author

Analysing the above advantages, we note that mobile apps and web platforms allow tourists and customers to conveniently book tours, hotels or restaurant tables online, without the need to contact agents or make calls. This greatly simplifies and speeds up the process. Interactive online platforms (Booking.com, Airbnb, OpenTable) allow customers to compare prices, conditions and availability in real time.

Chatbots and artificial intelligence (AI) automate responses to customer questions, providing 24/7 support. This significantly reduces the workload on staff and improves service levels.

Hotels and restaurants are already actively using AI-powered digital assistants to help guests with various issues, such as requesting additional services, menus, or information about local attractions.

The use of digital technologies in the travel and hospitality business has many advantages, but it also carries risks that can affect both businesses and consumers. One of the most significant is the technological risks associated with data security and the reliability of information systems [5]. The risk of leakage of personal information of tourists and customers (names, contacts, credit card details, travel history), hacker attacks on booking systems, CRM or payment services

can paralyse the operation of a hotel or travel company. Insufficient data protection can lead to loss of customer trust and legal liability under laws (e.g. GDPR in Europe).

Organisational challenges are also a significant risk of digital transformation. The introduction of new technologies requires significant changes in the structure and culture of enterprises, which can cause resistance from employees who are unwilling to adapt to new conditions or lack the necessary skills to work with these technologies. In addition, the digital transformation process requires investment in staff training, which increases costs [5].

"Economic risks are also an important aspect of digital transformation. Insufficient financial resources will lead to incomplete or inefficient implementation of digital solutions, which may ultimately fail to deliver the expected results" [14]. The introduction of new technologies (CRM, online booking systems, artificial intelligence, cyber defence) requires significant investment. Small and medium-sized businesses are often unable to finance these upgrades at the appropriate level. Due to incomplete or inefficient implementation of digital solutions, the expected results may not justify the costs. An incorrect assessment of the market or customer needs leads to poor technology choices. Digital technologies in the travel and hospitality industry significantly improve both the customer experience and the efficiency of operational processes. They enable the creation of personalised and convenient services, improve marketing, business management and optimise financial processes. With their help, businesses can not only attract new customers but also maintain the loyalty of existing ones by improving the quality of service.

Conclusions. As a result, it should be noted that in the modern digital economy, the introduction of digital technologies in the service sector is not just a trend, but a necessary prerequisite for the effective functioning of business. Analysis of the scientific and practical aspects of using tools such as artificial intelligence, big data, mobile applications, cloud services, CRM systems, AR/VR, Internet of Things and automation systems indicates their ability to significantly improve the quality of service, the level of personalization, consumer

convenience and business competitiveness. Digital solutions allow you to efficiently design customer experiences, optimize internal processes, reduce costs, and increase profitability at the same time. However, their implementation is associated with a number of difficulties, including economic risks, data protection issues and the need for qualified personnel. Therefore, the digital transformation of the service sector requires an integrated approach that combines innovative technologies, strategic vision, legal regulation and investments in human capital. The use of world experience, adapted to the national context, allows us to develop effective models of digital development of the service sector aimed at sustainable development and meeting the needs of modern consumers.

List of sources used

1. Kraus K. M., Kraus N. M., Marchenko O. V. Peculiarities of the application of digital technologies "Internet of Things" and the latest systems in business. *European Scientific Journal of Economic and Financial Innovation*. 2022. Vol. 1. № 9. P. 73–83. URL: https://journal.eae.com.ua/index.php/journal/article/view/150/131 (accessed 20.04.2025).

2. Verbivska L. V., Burynska O. I. The use of digital technologies in entrepreneurial activities. *Economy and society*. 2024. Vol. 61. URL: https://doi.org/10.32782/2524-0072/2024-61-84 (accessed 20.04.2025).

3. Borisov I. V. Service in the Conditions of Digital Technologies Use. *Law and Innovation Society.* 2021. № 2 (17). P. 187–191.

4. Zabashtanska T. V., Shpirnov I. L., Mykhailiuk M. T. Advantages and disadvantages of using modern digital technologies by participants in the financial services market. *Problems and Prospects of Economics and Management*. 2024. № 3 (39). P. 272–283.

5. Semchuk Zh. Role of Digital Technologies in the Transformation of Business Models of Modern Enterprises. *Academic visions*. 2024. Vol. 28. P. 1–8.

6. Balyk U. O., Loshenyuk I. R., Vayder T. M. On the role of digital technologies in the transformation of international marketing: challenges and prospects. *Topical issues of economic sciences*. 2024.

№ 1. URL: https://a-economics.com.ua/index.php/home/article/view/7/7 (accessed 20.04.2025).

7. Stashenko Y., Gavrylovskyi O. Implementation of digital transformation in trade and features of accounting. *Economy and society*. 2024. Issue 65. URL: https://economyandsociety.in.ua/index.php/journal/article/view/4380/4310 (accessed 20.04.2025).

8. Are there any prospects for the development of the service sector in Ukraine during the war? URL: https://hub.kyivstar.ua/articles/chy-ye-perspektyvy-dlya-rozvytku-sfery-poslug-v-ukrayini-pid-chas-vijnyhttps://hub.kyivstar.ua/articles/chy-ye-perspektyvy-dlya-rozvytku-sfery-poslug-v-ukrayini-pid-chas-vijny (accessed 20.04.2025).

9. What is the service sector? Service sector: definition of concept, profession and industry. URL: https://poradu.pp.ua/nauka/18080-schotake-sfera-obslugovuvannya-sfera-obslugovuvannya-viznachennya-ponyattya-profesyi-ta-galuz.html (accessed 20.04.2025).

10. Tourism statistics of Ukraine for 2024. URL: https://www.tourism.gov.ua/blog/u-2024-turistichna-sfera-ukrayini-prinesla-v-byudzhet-mayzhe-3-mlrd-grn (accessed 20.04.2025).

11. 5 Ways Disney Is Using AI. URL: https://digitaldefynd.com/IQ/ways-disney-use (accessed 20.04.2025).

12. Shanghai airport automates check-in with facial recognition. URL: https://apnews.com/general-news-travel-and-tourism-de81e35cf4ad4526b249e439a435f7e6 (accessed 20.04.2025).

13. Eco Friendly Safaris in Africa. URL: https://ecoadventuresafaris.com/eco-friendly-safaris-in-africa/ (accessed 20.04.2025).

14. Velychko K.Y., Tsybulska E.I. Transformation of Business Models of Companies: Modern Challenges and Prospects in the Digital Economy. Economy and society. Vol. 52. 2023. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2555/2474 (accessed 20.04.2025).

CHEVERDA Oleksandr,
PhD student at the Department of Economic Cybernetics,
Zaporizhzhia National University,
Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0009-0002-0812-8423

CHEVERDA Serhii,
PhD in Economics, Associate Professor,
Associate Professor at the Department of Economic Cybernetics,
Zaporizhzhia National University,
Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0000-0003-2161-037X

3.5. DIGITAL TECHNOLOGIES FOR MONITORING AND MANAGING LOGISTICS CHAINS IN CRISIS CONDITIONS: EU EXPERIENCE DURING THE PANDEMIC AND WAR IN UKRAINE

Introduction. Supply chain logistics in today's globalized world are becoming increasingly complex, integrated, and simultaneously vulnerable to various external influences. Recent years have demonstrated how quickly established logistics routes and processes can change under the influence of unpredictable global-scale crisis phenomena. The COVID-19 pandemic, which began in 2020, dealt an unprecedented blow to international logistics systems, causing border closures, port disruptions, container shortages, and rising transportation costs. In just the first year of the pandemic, container shipping costs increased by an average of 174 % according to the Drewry index [2], and in some directions – up to 400 %. Russia's military aggression against Ukraine in 2022 created a new set of challenges for global supply chains, particularly in the food, energy, and metallurgical sectors.

Under such crisis conditions, traditional approaches to logistics management prove insufficiently effective due to their inflexibility and low adaptability. The ability of logistics systems to rapidly reconfigure,

ensure transparency at all stages of the supply chain, and respond operatively to changes comes to the forefront. It is here that digital technologies demonstrate their transformational potential, providing tools for monitoring, analyzing, and managing logistics processes in real-time [1].

The experience of European Union countries, which faced the need for rapid adaptation of their logistics systems first to pandemic conditions and then to disruptions caused by military actions in Ukraine, is of particular interest for research. European companies actively implemented innovative digital solutions to ensure the resilience of their supply chains, which allowed them to minimize the negative consequences of crisis phenomena. According to research by consulting company McKinsey, European enterprises that invested in digitalization of logistics processes before the pandemic began were able to reduce the negative impact on their operations by an average of 35 % compared to companies that did not prioritize digital transformation [3].

Studying EU experience is particularly relevant in the context of finding ways to diversify logistics routes for Ukrainian exports, which faced unprecedented challenges due to the blockade of Black Sea ports and destruction of transport infrastructure. Before the start of the large-scale military invasion, about 90 % of Ukrainian agricultural and metallurgical exports were carried out through seaports. After their blockade, Ukrainian exporters were forced to reorient to land routes through EU countries, which led to an increase in logistics costs by an average of 40–150 % depending on the type of product and final destination.

Digital technologies offer a set of tools that can significantly optimize logistics planning and transportation execution processes under such complex conditions. Predictive analytics systems based on big data allow for anticipating potential bottlenecks and delays in supply chains. The Internet of Things (IoT) provides real-time cargo tracking, which is especially important when changing routes and modes of transport. Cloud platforms enable instant data updates and access to them by all participants in the logistics chain regardless

of their location. Blockchain technologies increase transparency and trust between partners, ensuring immutability of information about goods movement. Artificial intelligence systems optimize routes and resource planning, considering multiple variable factors.

According to the European Commission [1], about 71 % of EU logistics companies acknowledged that they accelerated their digital transformation plans as a result of the COVID-19 pandemic. As of the end of 2022, over 65 % of European enterprises had implemented at least one digital solution for monitoring and managing their supply chains, and 42 % use comprehensive digital platforms that integrate various functionalities. This trend continued to strengthen under the influence of new logistics challenges related to military actions in Ukraine.

Particularly important is the comparison of different approaches to digitalization of logistics processes that were applied in the EU during different types of crisis phenomena. While during the pandemic, the main focus was on ensuring uninterrupted supplies under quarantine restrictions and unstable demand, in the context of the Russian-Ukrainian war, priority issues became transport corridor security, route diversification, and reducing dependence on Russian energy sources. These differences determined different emphases in the use of digital tools.

The purpose of this study is to analyze the effectiveness of applying digital technologies for monitoring and managing logistics chains in crisis conditions based on the experience of EU countries during the COVID-19 pandemic and under conditions of the Russian-Ukrainian war.

Presentation of Main Research Results. The COVID-19 pandemic created unprecedented challenges for global supply chains, which were particularly acutely felt by European companies due to the high level of international integration of their logistics processes. The main problems faced by logistics systems during the pandemic were: border closures and movement restrictions; imbalance in the distribution of shipping containers; sharp fluctuations in demand for different categories of goods; disruption of supply regularity due to quarantine restrictions on production; labor shortages due to worker illness.

The complexity of these challenges required new approaches to logistics process management based on the use of digital technologies. Table 1 presents the main digital solutions that were implemented by European companies to overcome pandemic logistics challenges and their effectiveness.

Table 1

Effectiveness of Digital Technologies in Overcoming COVID-19 Pandemic Logistics Challenges in EU Countries

Digital Technology	Main Functions	Implementation Examples	Effectiveness (average indicator according to company assessments)
Predictive analytics based on Big Data	Demand forecasting, inventory optimization, identification of potential disruptions in supply chains	Nestlé (Switzerland/ EU), Unilever (Netherlands)	27 % reduction in demand forecast deviations, 18 % reduction in safety stock levels
Digital logistics platforms	Integration of all logistics chain participants, ensuring process transparency, document workflow automation	Maersk TradeLens (Denmark), Kuehne+Nagel (Switzerland/EU)	31 % reduction in administrative costs, 70 % acceleration of document processing
Internet of Things (IoT)	Real-time cargo tracking, goods condition monitoring, automatic status updates	DHL (Germany), CMA CGM (France)	43 % reduction in cargo loss cases, 54 % reduction in incident response time
Cloud logistics solutions	Ensuring remote access to logistics management systems, collaborative work of distributed teams	Geodis (France), DSV Panalpina (Denmark)	25 % increase in productivity under remote work conditions, 35 % reduction in coordination time
Blockchain technologies	Ensuring transparency and immutability of information, simplifying customs procedures	Port of Rotterdam (Netherlands), Carrefour (France)	65 % reduction in document verification time, 51 % reduction in fraud cases

Source: systematized by the author based on data from the European Logistics Association and company reports [6–9]

As shown in Table 1, digital platforms that integrate various functionalities and Internet of Things technologies demonstrated the highest effectiveness in overcoming pandemic logistics challenges. Digital platforms such as Maersk TradeLens [6] and Kuehne+Nagel Connect [4] allowed all participants in the logistics chain to be united in a single information space, ensuring process transparency and operational information exchange. This was especially important under constantly changing restrictions and regulations related to the pandemic.

Internet of Things technologies provided the ability to track cargo movement and condition in real-time, which allowed for quick response to delays and cargo redirection when necessary. For example, German logistics company DHL implemented the Smart Sensor IoT system, which not only tracked cargo location but also controlled temperature, humidity, and other parameters, which was critically important for transporting medical cargo and vaccines [5].

Particularly interesting is the example of implementing predictive analytics based on Big Data by European retailers. For instance, Dutch company Unilever used machine learning algorithms to analyze changes in consumer preferences during the pandemic and adjust their logistics processes according to new demand patterns. This allowed the company to reduce demand forecast deviations by 32 %, significantly exceeding the industry average (27 %) [7].

To visualize the dynamics of implementing various digital technologies in European companies' logistics processes during the COVID-19 pandemic, Figure 1 is presented.

As shown in Figure 1, all categories of digital technologies demonstrate significant growth in implementation levels after the COVID-19 pandemic began. The most substantial growth is observed in cloud logistics solutions (from 43 % to 78 %), which is explained by the need to ensure remote work for logistics departments and coordination of distributed teams under quarantine restrictions [8].

An important aspect of using digital technologies during the pandemic was their role in ensuring the resilience of medical goods and equipment supply chains.

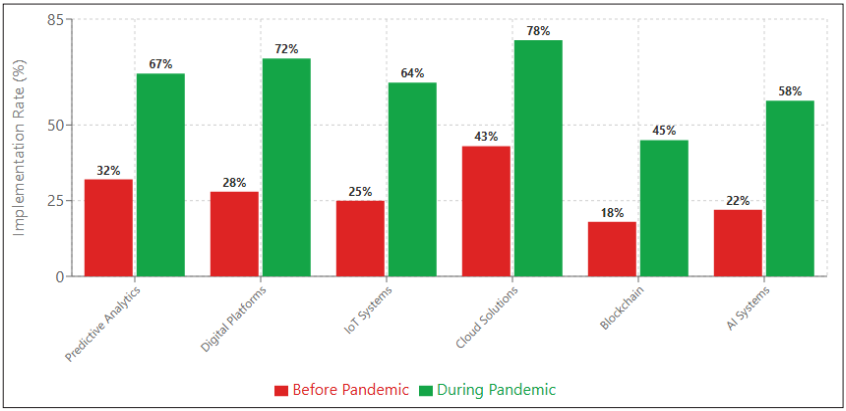

Fig. 1. Dynamics of Digital Technology Implementation in EU Companies' Logistics Processes Before and During COVID-19 Pandemic, %

The European Commission, in cooperation with logistics companies and medical equipment manufacturers, created the digital platform COVID-19 Clearing House for Medical Equipment, which allowed for coordinating the supply of critically important medical goods between EU member states [1]. The platform used artificial intelligence algorithms to optimize resource distribution according to each country's needs and available logistics capabilities.

The economic effect of implementing digital technologies in logistics processes during the pandemic can be assessed by comparing performance indicators of companies with different levels of digitalization. According to research by the European Logistics Association, companies with high levels of logistics process digitalization demonstrated 23 % better financial results during the pandemic compared to companies with low levels of digitalization. In particular, they were able to reduce logistics costs by an average of 15 %, decrease unsatisfied demand levels by 34 %, and accelerate order fulfillment by 29 % [3].

Russia's military aggression against Ukraine, which began on February 24, 2022, created fundamentally new challenges for European logistics systems that differed from problems caused by the

COVID-19 pandemic. Key among them were: blockade of Ukrainian Black Sea ports, through which up to 90 % of exports were carried out; destruction of transport infrastructure; need for urgent diversification of energy supply routes; increased security requirements for transport corridors; need for rapid reorientation of export and import flows.

For Ukrainian enterprises, these challenges proved particularly critical as they threatened the possibility of continuing export operations. At the same time, for European companies, they meant the need to find new sources of agricultural products, metals, and other goods traditionally imported from Ukraine, as well as developing new logistics routes to support the Ukrainian economy.

Table 2 presents a comparative analysis of changes in the structure of Ukrainian product exports by transport mode before and after the start of the large-scale invasion.

Table 2

Structure of Ukrainian Product Exports by Transport Mode, %

Transport Mode	Before War (2021)	After Port Blockade (2022–2023)	Change, p.p.
Maritime	90	5	–85
Railway	7	45	+38
Road	2	30	+28
River	1	20	+19

Source: calculated by the author based on data from the State Statistics Service of Ukraine and the Ukrainian Agribusiness Club

As shown in Table 2, there was a cardinal reorientation of export flows from maritime transport to railway, road, and river transport, which created unprecedented pressure on the corresponding infrastructure and required new approaches to organizing logistics processes. Under these conditions, digital technologies became a key tool for ensuring the efficiency of new logistics routes.

European companies actively implemented digital solutions to support Ukrainian exports and imports under war conditions. Digital platforms for coordinating multimodal transportation played a special

role, allowing the integration of different transport modes into unified logistics chains. For example, Polish logistics company PKP Cargo, in cooperation with Ukrzaliznytsia, developed the digital platform Rail Bridge, which optimized cargo transshipment processes at the border due to the difference in railway gauge [11].

To assess the effectiveness of various digital technologies in overcoming logistics challenges caused by the Russian-Ukrainian war, a survey of 150 European and Ukrainian logistics companies was conducted, the results of which are presented in Table 3.

As shown in Table 3, digital platforms for multimodal transportation (9.2 out of 10 points) and geospatial analytics systems (8.7 points) are rated highest for effectiveness. This is explained by the fact that these technologies directly solve the most critical challenges related to the need for rapid diversification of logistics routes and ensuring their security.

Table 3

Assessment of Digital Technology Effectiveness in Overcoming Russian-Ukrainian War Logistics Challenges

Digital Technology	Effectiveness Assessment (1–10 points)	Main Advantages	Main Limitations
1	2	3	4
Digital platforms for multimodal transportation	9.2	Ensuring seamless integration of different transport modes, optimization of transshipment processes	Require integration with existing management systems, high initial investments
Geospatial analytics systems	8.7	Determining optimal routes considering security risks, monitoring infrastructure condition	Require constant updating of infrastructure and security situation data
Blockchain solutions for customs clearance	8.5	Simplifying and accelerating customs procedures, ensuring transparency	Limited implementation at government level, compatibility issues between different systems

Continuation of Table 3

1	2	3	4
IoT cargo tracking systems	8.3	Real-time monitoring of cargo location and condition	Network coverage problems in certain regions, high equipment costs
Digital twins of logistics objects	7.6	Modeling and optimizing terminal and warehouse operations, capacity planning	Implementation complexity, high development costs
AI systems for risk forecasting	7.4	Identifying potential supply chain problems, recommendations for alternative routes	Limited forecast accuracy in highly uncertain conditions

Source: survey of European and Ukrainian logistics companies conducted by the author, n=150

Particular attention deserves the experience of applying digital technologies to optimize the Polish-Ukrainian border operation, which became a key transit hub for Ukrainian exports after the blockade of seaports. According to the Ministry of Infrastructure of Ukraine, waiting times for freight vehicles at the Polish border in the first months of the war reached 15–20 days, creating significant logistics delays and additional costs.

To solve this problem, the digital system e-Queue was implemented, which allowed optimization of the border crossing process for freight transport. The system is based on electronic queue technology using QR codes and online registration, allowing drivers to plan their arrival at the border and avoid long waits directly in the border zone [12]. The results of implementing the e-Queue system are presented in Figure 2.

Figure 2 shows that implementing the digital queue management system allowed reducing average waiting times at the border from 15–20 days to 3–5 days, significantly improving logistics operation efficiency.

An important aspect of digitalizing logistics processes under war conditions was implementing geospatial analytics systems to determine optimal routes considering security risks.

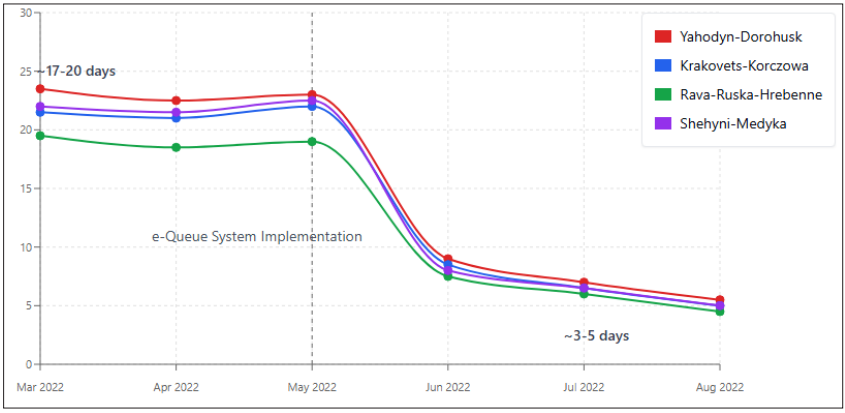

Fig. 2. Dynamics of Waiting Times at Polish-Ukrainian Border
Before and After e-Queue System Implementation, days

For example, Lithuanian company Traxus, together with Ukrainian partners, developed the Safe Route system, which uses data from various sources (including satellite images, social media information, and official reports) to assess the safety of different transport routes and adjust them in real-time [10].

To assess the economic effect of implementing digital technologies in Ukrainian enterprises' logistics processes under war conditions, an analysis was conducted of logistics cost changes for exporting various product types using alternative routes. The analysis results are presented in Table 4.

As shown in Table 4, implementing digital technologies allowed reducing logistics costs for exporting various product types by an average of 15.8–18.5 %. The greatest effect is observed for high-value products (sunflower oil, metal products), as reducing delivery time and increasing logistics process reliability is especially important for them.

It's important to note that the economic effect of implementing digital technologies manifests not only in reducing direct logistics costs but also in shortening delivery times, increasing supply reliability, and reducing risks. These factors are particularly significant under conditions of high uncertainty characteristic of wartime.

Table 4

Impact of Digital Technologies on Logistics Costs for Ukrainian Product Export via Alternative Routes, USD/ton

Product Type	Logistics Costs Before Digitalization	Logistics Costs After Digitalization	Cost Reduction, %	Main Implemented Technologies
Sunflower oil	110	90	18.2	Digital platforms for multimodal transportation, IoT tracking systems
Sunflower meal	95	80	15.8	Geospatial analytics systems, blockchain for customs clearance
Rapeseed oil	115	95	17.4	Digital platforms, risk forecasting systems
Grain crops	105	88	16.2	Digital platforms, IoT systems, blockchain
Metal products	135	110	18.5	Geospatial analytics systems, digital twins of terminals

Source: calculated by the author based on data from Ukrainian exporters, n=45

For a more detailed analysis of the impact of various digital technologies on logistics process efficiency, a regression analysis was conducted, the results of which are presented in Table 5.

The regression analysis results indicate that digital platforms for multimodal transportation (coefficient 0.42) and geospatial analytics systems (coefficient 0.35) have the greatest impact on reducing logistics costs. Meanwhile, blockchain solutions for customs clearance demonstrate the greatest impact on delivery time reduction (coefficient 0.45), which is explained by their ability to significantly accelerate border crossing and customs clearance processes [9].

The identified patterns allow formulating recommendations regarding priority directions for digitalizing logistics processes for different types of enterprises depending on their specific needs.

Table 5

Results of Regression Analysis of Digital Technology Impact on Logistics Process Efficiency

Digital Technology	Impact Coefficient on Logistics Cost Reduction	Impact Coefficient on Delivery Time Reduction	Statistical Significance (p-value)
Digital platforms for multimodal transportation	0.42	0.38	<0.001
Geospatial analytics systems	0.35	0.29	<0.001
Blockchain solutions for customs clearance	0.31	0.45	<0.001
IoT cargo tracking systems	0.28	0.32	<0.001
Digital twins of logistics objects	0.23	0.19	<0.05
AI systems for risk forecasting	0.27	0.34	<0.01

Source: author's calculations based on survey data from Ukrainian and European logistics companies

Integration into European Digital Logistics Ecosystems: Strategic Perspective for Ukrainian Enterprises

The experience of adapting logistics systems to COVID-19 pandemic conditions and the Russian-Ukrainian war demonstrates that the most effective approach to ensuring supply chain resilience is integration into broad digital ecosystems that unite various participants in logistics processes and ensure real-time data exchange [15]. In the context of deepening Ukraine's integration into the European economic space, the issue of Ukrainian enterprises joining European digital logistics ecosystems becomes particularly significant.

The European Union is actively developing several large-scale initiatives in the field of logistics digitalization that form a unified digital logistics space. Key among them are:

– *Digital Transport and Logistics Forum (DTLF)* – a platform for coordinating transport and logistics digitalization in the EU, uniting over 100 public and private organizations [13].

– *Electronic Freight Transport Information (eFTI)* – a system ensuring standardized digital information exchange about freight transportation between enterprises and government agencies [1].

– *European Maritime Single Window (EMSW)* – a single window for maritime transportation that simplifies documentation and procedures in EU ports [14].

– *Digital Services for Freight Transport Networks* – an initiative focusing on creating unified digital infrastructure for managing transport corridors [13].

To assess the readiness level of Ukrainian enterprises for integration into European digital logistics ecosystems, a survey of 120 Ukrainian exporting companies was conducted. The survey results are presented in Figure 3.

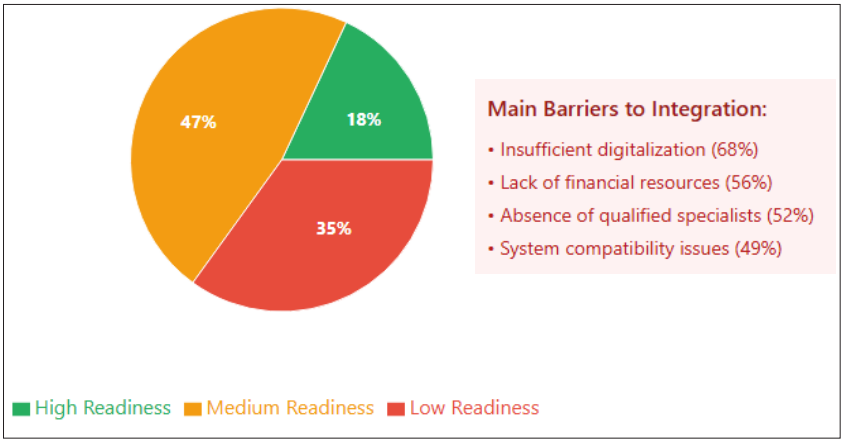

Fig. 3. Readiness Level of Ukrainian Enterprises for Integration into European Digital Logistics Ecosystems, %

Figure 3 shows that only 18 % of Ukrainian enterprises assess their readiness level for integration into European digital logistics ecosystems as high. Most companies (47 %) characterize their

readiness as medium, and 35 % as low. Respondents named the main barriers to successful integration as: insufficient level of internal process digitalization (68 %), lack of financial resources for digital technology investments (56 %), absence of qualified specialists (52 %), insufficient compatibility of existing systems with European standards (49 %).

Based on the analysis of European experience and assessment of Ukrainian enterprises' readiness, a model for gradual integration into European digital logistics ecosystems was developed (Figure 4).

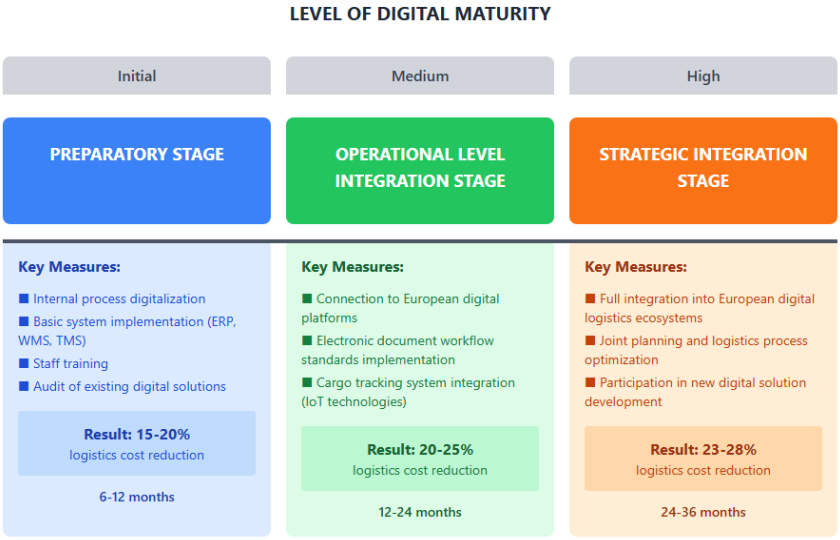

Fig. 4. Model for Gradual Integration of Ukrainian Enterprises into European Digital Logistics Ecosystems

The proposed model includes three main stages:

– preparatory stage – digitalization of enterprise internal processes, implementation of basic digital solutions (ERP, WMS, TMS systems), staff training;

– operational level integration stage – connection to European digital platforms for multimodal transportation, implementation

of electronic document workflow standards, integration of cargo tracking systems;

– strategic integration stage – full integration into European digital logistics ecosystems, joint planning and optimization of logistics processes, participation in developing new digital solutions.

For each stage, key technologies, necessary resources, and expected results are defined, allowing enterprises to plan the digital transformation process according to their capabilities and needs.

According to expert estimates, successful integration of Ukrainian enterprises into European digital logistics ecosystems will allow reducing logistics costs by an average of 23–28 % compared to the current level, shortening delivery time by 30–35 %, and increasing supply reliability by 40–45 %. These improvements will have a significant impact on Ukrainian product competitiveness in European markets [1].

Given the strategic importance of digitalizing logistics processes for ensuring Ukraine's integration into the European economic space, it is advisable to implement government support programs for digital transformation of logistics systems. Such programs may include:

– financial support (grants, preferential loans) for implementing digital technologies in Ukrainian enterprises' logistics processes;

– training programs for preparing specialists in digital logistics;

– promoting Ukrainian companies' participation in European logistics digitalization initiatives;

– harmonization of Ukrainian standards with European ones in the field of digital document workflow and logistics information exchange;

– development of digital infrastructure to ensure reliable functioning of logistics information systems.

An important aspect of ensuring logistics process efficiency is the interaction between digital technologies and physical infrastructure. In the context of post-war recovery of Ukraine, the issue of integrating digital solutions into transport infrastructure reconstruction strategies becomes particularly relevant.

Analysis of European experience demonstrates that the most effective approach is the "digital-first" concept, when planning and

implementing infrastructure projects is carried out considering future digital solutions that will be based on them [15]. In particular, when reconstructing Ukraine's transport infrastructure, it is advisable to immediately provide for:

– deployment of IoT sensor networks for monitoring infrastructure object conditions;

– implementation of artificial intelligence-based transport flow management systems;

– creation of digital twins of transport infrastructure for modeling and optimizing its use;

– development of charging station networks for electric transport with integrated digital management systems;

– implementation of intelligent border infrastructure management systems.

According to expert estimates, integrating digital technologies into transport infrastructure reconstruction processes will allow increasing its efficiency by 25–30 % compared to traditional approaches, as well as ensuring faster adaptation to changes in logistics needs.

To determine priority directions for integrating digital technologies into Ukraine's transport infrastructure reconstruction processes, an expert survey was conducted, the results of which are presented in Table 6.

Table 6

Priority Directions for Integrating Digital Technologies into Ukraine's Transport Infrastructure Reconstruction

Direction	Priority (1–10 points)	Expected Impact on Logistics Process Efficiency
1	2	3
Digitalization of border infrastructure	9.4	60–70 % reduction in border crossing time, 40–50 % increase in throughput capacity
Intelligent railway network management systems	9.1	35–40 % increase in rolling stock utilization efficiency, 25–30 % reduction in delivery time

Continuation of Table 6

1	2	3
Digital solutions for multimodal logistics hubs	8.8	45–50 % acceleration of transshipment processes, 30–35 % increase in infrastructure utilization coefficient
Intelligent transport systems for highways	8.5	20–25 % increase in throughput capacity, 15–20 % reduction in transportation time
Digital infrastructure condition monitoring systems	8.2	25–30 % reduction in infrastructure maintenance costs, 30–35 % increase in transportation safety
Digital solutions for river transport corridors	7.9	30–35 % increase in river transport utilization efficiency, integration into multimodal transportation

Source: expert survey results, n=35 (experts in logistics, transport infrastructure, and digital technologies)

As shown in Table 6, digitalization of border infrastructure has the highest priority, reflecting the critical role of border crossings in ensuring Ukrainian economy export operations under conditions of seaport blockade. Intelligent railway network management systems and digital solutions for multimodal logistics hubs also have high priority, emphasizing the importance of these transport infrastructure elements for ensuring efficient alternative logistics routes.

Based on the conducted analysis, a conceptual model of synergy between digital technologies and Ukraine's transport infrastructure reconstruction strategy can be proposed (Figure 5).

The proposed model provides for interconnected development of physical infrastructure and digital solutions that ensure its efficient use. Key elements of the model are:

a) digital twins of infrastructure objects – virtual models that allow planning and optimizing infrastructure reconstruction and operation processes;

b) integrated logistics platforms – digital solutions that ensure coordination of different transport modes and logistics process participants;

c) IoT-based monitoring and management systems – networks of sensors and actuators that ensure data collection about infrastructure condition and remote management capabilities;

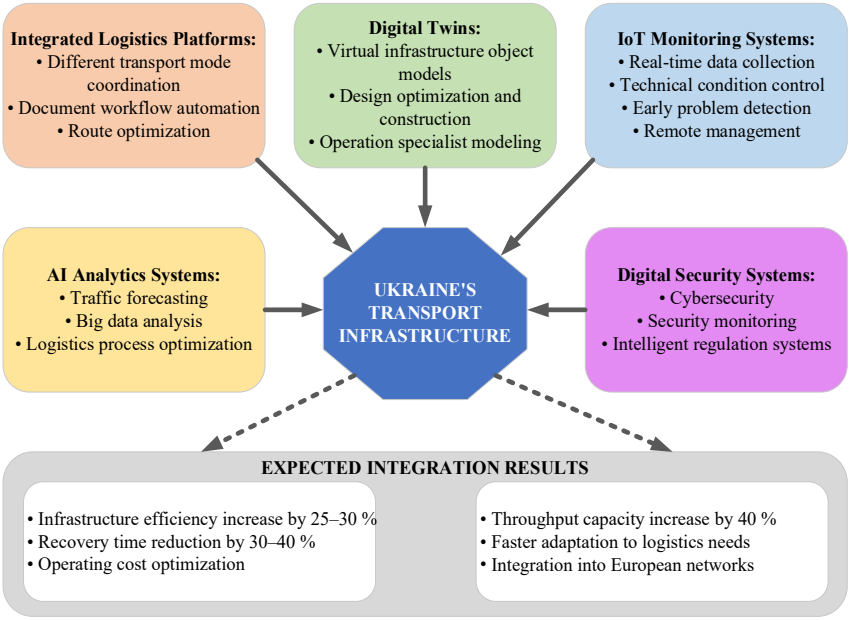

Fig. 5. Conceptual Model of Synergy Between Digital Technologies and Ukraine's Transport Infrastructure Reconstruction Strategy

d) AI-based analytical systems – solutions that analyze large volumes of data to optimize logistics processes and predict potential problems;

e) digital security systems – technologies that enhance transport infrastructure and logistics process security.

Implementing this model requires coordinating efforts of the state, business, and international partners, as well as significant investments.

At the same time, it will allow creating a modern, efficient, and resilient transport-logistics system that will ensure Ukrainian economy competitiveness in the global context.

Conclusions. The conducted study of digital technologies for monitoring and managing logistics chains in crisis conditions allows drawing several important conclusions regarding their role in ensuring logistics system resilience and prospects for their implementation in the Ukrainian economy.

Analysis of EU countries' experience during the COVID-19 pandemic demonstrated that digital technologies became a key factor in adapting logistics systems to unprecedented challenges related to quarantine restrictions, supply chain disruptions, and sharp changes in consumer demand. Digital platforms that integrate various functionalities and unite all logistics chain participants in a unified information space proved most effective. Such platforms allowed reducing administrative costs by an average of 31 % and accelerating document processing by 70 %. Internet of Things technologies also demonstrated high effectiveness, ensuring real-time cargo tracking and reducing cargo loss cases by 43 %.

The Russian-Ukrainian war created fundamentally new challenges for logistics systems that differed from pandemic-caused problems. The blockade of Ukrainian Black Sea ports, through which up to 90 % of exports were carried out, necessitated cardinal reorientation of export flows to railway (share growth from 7 % to 45 %), road (from 2 % to 30 %), and river (from 1 % to 20 %) transport. Under these conditions, digital technologies became a key tool for ensuring new logistics route efficiency. Digital platforms for multimodal transportation (rating 9.2 out of 10 points) and geospatial analytics systems (8.7 points) demonstrated the highest effectiveness in overcoming Russian-Ukrainian war logistics challenges. Regression analysis showed that digital platforms for multimodal transportation (coefficient 0.42) and geospatial analytics systems (coefficient 0.35) have the greatest impact on reducing logistics costs, while blockchain solutions for customs clearance have the greatest impact on delivery time reduction (coefficient 0.45).

Implementing digital technologies in Ukrainian enterprises' logistics processes allowed reducing logistics costs for exporting various product types by an average of 15.8–18.5 %. The greatest effect is observed for high-value products (sunflower oil, metal products), as reducing delivery time and increasing logistics process reliability is especially important for them.

Analysis of Ukrainian enterprises' readiness level for integration into European digital logistics ecosystems showed that only 18 % of companies assess their readiness level as high, while most (47 %) characterize it as medium, and 35 % as low. Main barriers to successful integration are insufficient level of internal process digitalization (68 %), lack of financial resources for digital technology investments (56 %), absence of qualified specialists (52 %), and insufficient compatibility of existing systems with European standards (49 %).

To ensure successful integration of Ukrainian enterprises into European digital logistics ecosystems, a gradual integration model is proposed, including a preparatory stage (internal process digitalization), operational level integration stage (connection to European digital platforms), and strategic integration stage (full integration into European digital logistics ecosystems). Successful implementation of this model will allow reducing logistics costs by an average of 23–28 % compared to the current level, shortening delivery time by 30–35 %, and increasing supply reliability by 40–45 %.

Under conditions of post-war recovery of Ukraine, the issue of integrating digital solutions into transport infrastructure reconstruction strategies becomes particularly relevant. The most effective approach is the "digital-first" concept, when planning and implementing infrastructure projects is carried out considering future digital solutions. The highest priority is digitalization of border infrastructure (9.4 out of 10 points), intelligent railway network management systems (9.1), and digital solutions for multimodal logistics hubs (8.8).

Based on the conducted research, the following recommendations can be formulated for different stakeholders:

For Ukrainian enterprises:

– accelerate digitalization of internal logistics processes, starting with implementing basic systems (ERP, WMS, TMS);

– invest in connecting to European digital logistics platforms, especially those specializing in multimodal transportation;

– develop staff competencies in digital logistics and supply chain management;

– implement IoT-based cargo tracking technologies to ensure logistics process transparency;

– use blockchain solutions to simplify and accelerate customs procedures.

For Ukrainian government agencies:

– develop and implement a state program supporting logistics process digitalization in the Ukrainian economy;

– ensure harmonization of Ukrainian standards with European ones in digital document workflow and logistics information exchange;

– integrate "digital-first" principles into transport infrastructure reconstruction strategies;

– prioritize border infrastructure digitalization to increase throughput capacity and reduce border crossing time;

– promote Ukrainian companies' participation in European logistics digitalization initiatives.

For international partners and organizations:

– provide technical and financial support for logistics process digitalization in Ukraine;

– promote integration of Ukrainian enterprises into European digital logistics ecosystems;

– ensure knowledge and technology transfer in digital logistics;

– invest in digital infrastructure development to ensure reliable functioning of logistics information systems.

Implementing these recommendations will allow increasing efficiency and resilience of logistics systems in Ukraine, promote Ukrainian economy integration into the European economic space, and ensure Ukrainian enterprises' competitiveness in international markets under unprecedented challenges caused by Russian military aggression.

List of sources used

1. European Commission. Digital transformation of logistics in the EU: trends and challenges. *European Commission.* 2021. URL: https://ec.europa.eu/info/publications/digital-transformation-logistics_en.

2. Drewry J. Drewry Container Freight Rate Insight: Impact of COVID-19 on global container shipping. *Drewry Maritime Research.* 2020. URL: https://www.drewry.co.uk.

3. McKinsey & Company. How COVID-19 is reshaping supply chains and logistics. *McKinsey & Company.* 2021. URL: https://www.mckinsey.com/industries/transportation-and-logistics/our-insights/how-covid-19-is-reshaping-supply-chains-and-logistics.

4. Kuehne+Nagel. Digital platforms for global logistics: Driving the future of supply chain management. *Kuehne+Nagel.* 2020. URL: https://www.kuehne-nagel.com.

5. DHL. Smart sensor IoT technology for real-time cargo tracking. *DHL Logistics.* 2020. URL: https://www.dhl.com.

6. Maersk. Maersk TradeLens: Digitalization of shipping through blockchain technology. *Maersk*. 2020. URL: https://www.maersk.com.

7. Unilever. Using machine learning to predict demand and optimize logistics during the COVID-19 crisis. *Unilever*. 2020. URL: https://www.unilever.com.

8. Geodis. The rise of cloud-based logistics platforms and remote working solutions. *Geodis*. 2021. URL: https://www.geodis.com.

9. Port of Rotterdam. Blockchain solutions for customs procedures and transparency. *Port of Rotterdam.* 2020. URL: https://www.portofrotterdam.com.

10. Traxus. Safe Route: Using geospatial analytics to optimize transport routes in conflict zones. *Traxus*. 2022. URL: https://www.traxus.com.

11. PKP Cargo. Rail Bridge: Digital solutions for optimizing cross-border cargo transport. *PKP Cargo*. 2022. URL: https://www.pkp-cargo.pl.

12. Ministry of Infrastructure of Ukraine. E-Queue: Digitalization of border crossing for freight vehicles. *Ministry of Infrastructure of Ukraine.* 2022. URL: https://www.mtu.gov.ua.

13. Digital Transport and Logistics Forum. EU initiatives for digital logistics. *DTLF*. 2021. URL: https://www.dtlforum.eu.

14. European Maritime Single Window. Simplifying port documentation and procedures through digital solutions. *EMSW*. 2021. URL: https://www.emsw.eu.

15. World Bank. Supply Chain Digitalization for Crisis Management: Lessons Learned from COVID-19. *World Bank Group.* 2021. URL: https://www.worldbank.org.