CHAPTER 2.
THE IMPACT OF DIGITALIZATION ON THE SOCIO-ECONOMIC SECURITY OF EUROPEAN COUNTRIES AND UKRAINE

KALIUZHNA Yuliia Viktorivna,
Candidate of Economic Sciences, Associate Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0000-0002-3335-6551

CHEREP Oleksandr Grigorovich,
Doctor of Economics, Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0000-0002-3098-0105

2.1. THE IMPACT OF DIGITALIZATION ON THE SOCIO-ECONOMIC SECURITY OF EUROPEAN COUNTRIES AND UKRAINE

Introduction. Digitalization is an important factor in modern social and economic development, as its impact is visible in all spheres of life – from business and education to public administration. The introduction of digital technologies contributes to increased productivity, optimization of business processes, development of e-government and improvement of the quality of life of the population. At the same time, digital transformation is radically changing the labor market, methods of communication and mechanisms of doing business, which significantly affects the socio-economic security of states. It, in turn, covers both economic

indicators, namely employment, income level, competitiveness of the economy, and social factors – accessibility of education, medicine, social protection. Successful digitalization contributes to increasing socio-economic security through automation of processes, development of digital services and creation of new opportunities for citizens and businesses, which were studied by scientists: Brown T., Mann B., Ryder N., Subbia M., Kaplan J., Dhariwal P. [1], Khalid M., and Yusaf M. M. [2], Prakash D. [3], Garcia K. [4], Jordan M. I., and Mitchell T. M. [5], Oleinikova L. G., Savenko D. M., Kolisnyk K. A. [6], Cherep A. V. [7–10], Cherep O. G. [7; 9], Gelman V. M., Loseva E. S. [7], Dashko I. M. [8; 9], Ogrenych Yu. O. [8–10], Oleinikova L. G., Vasylenko D. O. [10].

At the same time, digital transformation carries certain risks, including the growth of cyber threats, increasing digital inequality and dependence on global technology corporations. European countries are leaders in the implementation of digital technologies, implementing comprehensive digitalization strategies to increase competitiveness and security. Ukraine is not lagging behind them, but on the contrary is actively implementing digital reforms, in particular in the areas of e-government, banking technologies and e-commerce. However, on the path to digital transformation, the country faces certain problems, including: uneven access to digital technologies, low level of cybersecurity and insufficient readiness of the labor market for changes.

Presentation of the main research material. Due to the ambiguity of interpretations and a wide range of contexts, the concept of “digitalization” still remains a subject of ambiguous understanding and application, especially in the legal sphere and the activities of executive authorities in Ukraine. This situation often arises due to confusion with the concepts of “digitization” and “digitalization”, which are often used as synonyms for digitalization, although they have significant differences. In particular, digitization

and digitalization involve the conversion of analog data into digital format, while digitalization covers a much wider range of changes, including the transformation of business processes and the modernization of society through the use of digital technologies. An additional problem is the perception of digitalization exclusively through the prism of technology or the reduction of its essence to the simple conversion of paper documents into digital form. Such a superficial understanding leads to a narrow approach that ignores key aspects of digital transformation – changes in management, organizational culture, business development strategy, communications and other important areas.

In this context, it is important to pay attention to the research of K. V. Nychiporenko and M. V. Aleksandrova, who, analyzing the benefits of digitalization, also focus on its risks, such as digital inequality and discrimination, which are significant deterrent and preventive factors. As well as the presentation of the perception of digitalization through such trivial things as "leadership", "trust", "a person of the new generation", etc., similar to the imposition of elements of indoctrination – "uncritical perception by social subjects of ideas proposed from the outside, the purposeful implementation of certain political ideas to form a certain public consciousness" [12]. Thus, digitalization is a complex and multifaceted process that goes far beyond the implementation of technologies, it covers not only technical aspects, but also significant social, economic and legal changes. This is not just the integration of innovative solutions, but a profound transformation that affects the structure and principles of functioning of state institutions, the economy, and society as a whole. Its role cannot be ignored, as it shapes the country's position in the global economic space. The COVID-19 pandemic and military operations in Ukraine have become particularly significant catalysts for digital transformation, accelerating the introduction of digital solutions into all aspects of life. In the era of globalization, the digital economy is becoming increasingly important for

the development of states. It is important to realize that it is not a separate industry, but an integrated digital environment that changes traditional economic models. The boundary between the classical and digital economies is gradually blurring, which makes it difficult to distinguish them. Digitalization is the driver of modern social development, contributing to the modernization of all spheres of activity, in particular the labor market and economic processes. Investments in digital technologies demonstrate significantly higher profitability compared to traditional areas. The rapid development of information technologies is fundamentally changing the way people live, gradually introducing digital solutions into all spheres of activity. Government institutions, the business environment, and citizens are actively using technologies such as artificial intelligence, robotics, cyber systems, big data, blockchain, paperless technologies, cloud computing, 3D printing, unmanned systems, biometrics, and quantum technologies. Digitization of economic processes brings significant benefits, including:

For society:

– increasing economic and social effects from the use of digital technologies;
– improving the quality of life of citizens;
– increasing labor productivity;
– creating new profitable business models;
– effective monitoring of economic processes.

For businesses:

– minimizing the involvement of intermediaries or the possibility of selling directly to consumers;
– reduction of operating costs;
– improving business communications;
– quick feedback from customers;
– creating new products and services that meet market demands.

For consumers and employees:

– reducing the cost of goods and services by optimizing logistics and production processes;

– global availability of goods and services regardless of geographical location;

– personalization of offers that better meet customer needs.

Despite its numerous advantages, digitalization is also accompanied by certain threats, including:

a) cyber risks:the risk of unauthorized access, cyberterrorism, personal data leakage;

b) social challenges: automation can lead to job losses and increased unemployment;

c) privacy issues: digital control and monitoring of the population;

d) technical threats: Internet connection instability, which may affect access to digital services.

Despite certain shortcomings, the digital economy contributes to the reduction of social barriers and creates equal opportunities for all. Remote employment eliminates gender discrimination, since the productivity of an employee is assessed not by secondary characteristics, but by his skills and work results. In particular, the opportunity to work online opens up new prospects for women, housewives, and other social groups who previously had limited access to quality jobs. In addition, digitalization provides ample opportunities for distance learning, development of professional skills, access to the global labor market and information. This allows people to effectively realize their own potential and improve their financial situation.

The practical implementation of electronic technologies in the sphere of public administration in Ukraine started in 2016 with the approval of the Concept of the Development of the Electronic Services System. Its main goal was to determine strategic directions, mechanisms and time frames for creating an effective system of electronic services that would meet the needs of individuals and legal entities. The main principles of this system included accessibility, transparency, security, absence of corruption risks, cost minimization and efficiency. According to the plans, by 2020, it was planned to fully

ensure the electronic provision of services in all spheres of public life, the implementation of integrated and cross-border electronic services. However, due to a number of factors, in particular the lack of political will, some of the planned initiatives were never fully implemented. The key tool for the implementation of electronic services was e-government (electronic governance), the conceptual basis of which was formed by the theories of the information society that became widespread in the second half of the 20th century.

The use of electronic governance mechanisms can significantly improve the quality of service to citizens and businesses, make the activities of state bodies more open, transparent and efficient. It is important to understand that e-government is not just a modern management tool, but a new approach to public administration, which involves the automation of administrative processes, digital interaction between authorities, business and citizens, as well as the performance of its functions by the state using digital technologies. According to the Concept of the Development of Electronic Governance, this system has become one of the priority areas of public administration reform. It was assumed that its development would be transformative and even revolutionary in nature, aimed at:

– optimization of e-government functionalities;

– reducing costs for government agencies through digitalization of processes;

– introduction of innovative methodologies and technologies to improve the efficiency of public administration.

To achieve these goals, a set of strategic measures was identified, including the modernization of public services and the digital integration of interaction between the state, citizens and business. Particular attention was paid to digitalization in the field of social protection of the population, which provided for:

1. Creation of a single state register of the social sphereand unifying existing disparate databases for more efficient management of social benefits.

2. Implementation of electronic sick leave, which allows you to reduce bureaucratic procedures and increase convenience for citizens.

3. Automation of data verification when assigning social benefits and benefits, which minimizes possible abuses and increases the speed of processing applications.

4. Introduction of electronic employment contracts, which simplifies the employment process and promotes transparency in labor relations.

One of the key tools for implementing the Strategy should be the information system – the Unified Information System of the Social Sphere (hereinafter referred to as the EISSS).

This is a joint project of the Ministry of Social Policy and the Ministry of Digital Economy, an expansion and continuation of the updated project "E-Social", which was created taking into account the latest information and management technologies, unified modern standards of quality of service to citizens, with the possibility of making effective organizational and structural decisions. The EISSS is being created on the technological basis of information systems and registers of the social sphere that are already in operation, in particular the Register of Insured Persons of the Pension Fund (RZO), with full integration with the Unified State Web Portal of Electronic Services "Diya" [13]. With the help of the EISSS, the digitalization of the social sphere will cause global changes in the organization, management and provision of social services. The main innovation will be the creation of a unified social register, which will be formed on the basis of the register of insured persons.

This integrated system will accumulate data on all citizens receiving social support, as well as provide complete and up-to-date information on all payments made and benefits assigned. An important step will be to merge data from disparate social registries into a single digital ecosystem. This will ensure the automation and centralization of social processes, eliminating

duplication of administrative procedures and the need for numerous local social security offices. Digitalization of the social sphere is beneficial for both citizens and the state. For citizens personally, it means a convenient and accessible service, the ability to receive a service (payment) in a few minutes without leaving home, which will also help overcome corruption. For the state, digitalization will allow for the optimization of expenditures, in particular by streamlining payments, transparent control over them, as well as reducing administrative costs and bureaucracy, along with a complete transition to electronic document management.

Developed countries of the world in the conditions of the modern economy pay considerable attention to digital transformation. In particular, in 2010, the European Union countries launched the strategic initiative Digital Order, which defined key measures to achieve the set goals by 2020. One of the main components of this initiative was the formation of the Digital Single Market.

To assess the level of technological development and implementation of digital innovations in EU countries, a special indicator is used – the DESI Index. This index includes five main sub-indices: development of digital infrastructure, level of digital skills of the population, activity of Internet use, integration of digital technologies into the business environment and development of e-government.

A component of the DESI index is the digital capital indicator, which is based on five key parameters grouped into two main categories. One of them analyzes the basic digital skills of the population, while the other assesses the level of preparation of graduates of educational institutions for work in the digital environment. According to the results of this index for 2020, the leaders of the European Union in the field of digital technologies were countries such as the Netherlands, Belgium, Luxembourg, Denmark, Finland, Sweden, Ireland, the United Kingdom, Austria and Estonia (Fig. 1).

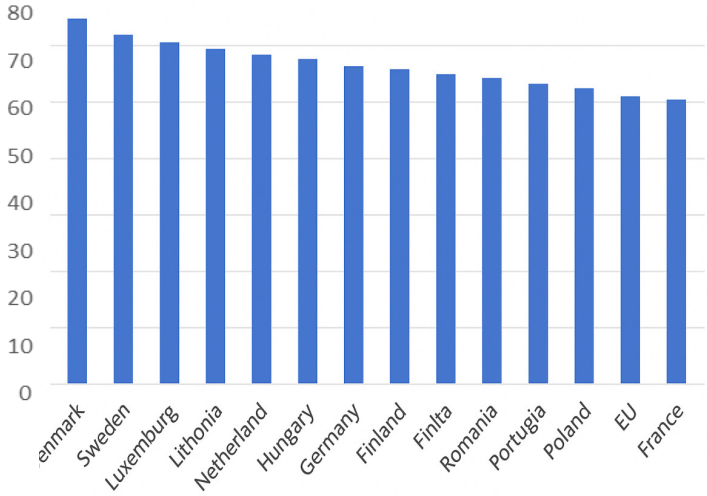

Fig. 1. Score indicator of the rating level of communication accessibility in EU countries in 2020

According to the 2020 DESI Report, the coverage of households in the European Union with next-generation networks increased from 83% to 86%. The share of households with access to fixed broadband networks also increased from 15% to 26%. Almost the entire EU population (96%) is covered by the 4G network, while the level of 5G coverage remains relatively low at around 25%. The countries with the highest level of digital readiness have strong information and communication capabilities. Among them are Finland, Germany, Hungary and Italy. The leaders in terms of digital accessibility are Denmark, Sweden and Luxembourg, where DESI index indicators are in the range of 65–68 points. On average, the average level of digital accessibility in EU countries is 50 points, while the lowest indicators are observed in Bulgaria, Cyprus and Greece.

Actively modernizing the educational process, the European Union countries are forming a strategy for the development of education,

implementing the results of scientific research, taking into account innovative digitalization programs. It is the implementation of digital innovative technologies that allows for the implementation of many European grants that support Ukrainian educators during the Russian-Ukrainian war. The formation of the Digital Education Action Plan for 2021–2027 allows for the implementation of domestic initiatives, taking into account European experience.

This Plan:

– Forms a long-term vision for high-quality, accessible and inclusive digital education in Europe.

– Analyzes the challenges and opportunities that have arisen as a result of the COVID-19 pandemic, when technology has played a major role in enabling continuous learning.

– Emphasizes the need for enhanced cooperation between EU countries in the field of digital education and emphasizes the importance of intersectoral interaction for the effective implementation of digital solutions in the educational process.

– It provides a wide range of opportunities, including improving the quality of digital teaching, supporting the digitalization of pedagogical methods and learning approaches, and providing the necessary infrastructure for inclusive and sustainable distance learning.

This document builds on the previous 2018–2020 plan, which was developed to support distance learning during the pandemic. It was then that the first steps were identified to adapt educational institutions and national education systems to rapid digital change.

The new plan has two strategic priorities: 1) promoting the development of a highly effective digital education ecosystem; 2) enhancing digital skills and competencies for the digital transformation of education.

Priority 1: Promoting the development of a high-performance digital education ecosystem includes:

– infrastructure, connectivity and digital equipment;

– effective planning and development of digital potential, along with modern organizational capabilities;
– digitally competent and confident teachers and educational staff;
– high-quality educational content, user-friendly tools, and secure platforms that adhere to digital privacy rules and ethical standards.

Priority 2: Improving digital skills and competencies for digital transformation involves:
– basic digital skills and competencies from an early age;
– digital literacy, including combating disinformation;
– computer education;
– good knowledge and understanding of artificial intelligence (AI) technologies;
– advanced digital skills, increase in IT specialists;
– ensuring equal participation of girls and young women in digital research and careers (European Commission, 2021) [15].

Currently, digitalization has not yet had a significant impact on improving the operational efficiency and overall profitability of most enterprises in Ukrainian sectors of the economy. The only exceptions are such industries as trade, where e-commerce is actively developing, administrative services thanks to the introduction of e-government, and information technologies, where the development and integration digital technologies are an integral part of the evolutionary process. However, digitalization in these industries causes contradictory results, which concern both the use of Ukraine's competitive advantages in the international economic space and ensuring stable socio-economic development. It is important to note that the main growth is observed mainly in the extractive industry, much smaller – in the manufacturing industry, and even less pronounced – in mechanical engineering.

It is important to note that there is a slowdown in production volumes over the 10 months of 2021. However, there is an increase in services provided in terms of the volume of exports of IT services, the volume of taxes paid by the IT sector

to the budget, and the volume of investments attracted to the IT sector (Table 1) [16].

Table 1

Volumes of IT sector activity in Ukraine for 2016–2020 [16]

Indicators	2016	2017	2018	2019	2020
Volume of IT services exports, million USD	1,975	2,485	3,204	4,173	5,026
The amount of taxes paid by the IT sector to the budget, UAH million	7,117	9,642	13,048	16,697	1,155
The volume of investments attracted to the IT sector, million USD	80	265	345	544	571

Within the framework of the EU4Digital program, which supports the harmonization of digital markets among the Eastern partners, several pilot initiatives are being implemented in Ukraine, such as eDelivery, eCustom, eCommerce, which will become available to all Ukrainian companies in the near future. These initiatives will contribute to the acceleration of digital transformations in the country's economy. The Ministry of Infrastructure of Ukraine is working on issues related to e-commerce, and the National Commission for Regulation of Communications and Informatization provides standards for postal services. Both international standards (UPU) and national ones are being implemented in Ukraine. We believe that the introduction of a data exchange system based on digital technologies into the activities of domestic businesses allows for beneficial relationships with foreign partners, in particular European ones, which will avoid traditional problems associated with paper red tape, delays and risks of loss or leakage of confidential information when it is transmitted by mail. The eDelivery pilot project, for example, was tested on the Ukraine-Poland route, where a Ukrainian exporter sends an electronic invoice through a national access point,

and it then arrives at a Polish company through a Polish access point in the Peppol network. The eCustom pilot project has also been launched, which is aimed at combating shadow customs schemes, where, for example, an empty truck can leave one country and not reach another country or arrive with goods. Thanks to electronic data exchange, customs authorities will be able to quickly detect and block such violations. The eCommerce initiative aims to increase trade volumes between countries using digital platforms. Companies will be able to sell their goods on the markets of the EU and other countries, placing the necessary information on generally accepted trading platforms. A special feature is the work of postal operators, who must deliver shipments from Ukraine to the EU within 24 hours from the moment of acceptance. Of course, these factors positively characterize the processes of digitalization in Ukraine. However, the success of these initiatives largely depends not on existing support, but rather on overcoming it, in particular regarding the institutional environment and legislative support. The digital development of Ukraine is significantly slowed down due to imperfect management of the national economy, the inconsistency of current legislation with the requirements of digital changes, the lack of appropriate legal institutions and procedures for regulating relations and protecting rights in conditions of rapid socio-economic transformations. This is especially noticeable when analyzing the path that Ukraine is taking to building a developed information society.

Cyber threats in the financial sector cover a wide range of dangers that can cause significant financial losses and damage the reputation of financial institutions among customers. The list of main cyber threats:

– Phishing is the process of providing customers with false information aimed at soliciting reliable information about confidential payment card data.

– There are also processes of distributing programs that are aimed at damaging the computer systems of banks and other financial institutions in order to obtain reliable information about their activities.

– DDoS attacks are attempts by attackers to overload a financial institution's website by using hacked servers, making the site inaccessible due to excessive load on the servers.

– Intelligence involves collecting confidential data about financial institutions and their customers in order to further implement cyberattacks using previously obtained information.

– Information interception is carried out using spyware that monitors and receives data transmitted over the network.

– Skimming involves installing special devices on ATMs or payment terminals that allow criminals to steal information entered by users, including credit card numbers or PIN codes.

– There is also cyber espionage, which is aimed at obtaining confidential information about the activities of financial and non-financial institutions through illegal means.

– Fraud also has a fairly wide range of uses of digital technologies to obtain reliable information about the activities of individuals and legal entities in order to use this information for further criminal use.

However, this list is not exhaustive, as the development of new technologies and the emergence of social challenges force cybercriminals to create new ways of fraud. Despite the complexity of methods for penetrating organizational networks, a significant proportion of security incidents arise from internal threats, in particular from current or dismissed employees, as well as from unintentional errors of personnel. According to research, insider attacks are 48% more difficult to detect and prevent than external cyberattacks. Another common type of cybercrime is cryptocrime. More and more financial services include cryptocurrency transactions, which attracts crypto enthusiasts, but such services are not without significant risks, as their systems usually do not have adequate protection and have not undergone extensive testing [17].

Encryption, which is used in the development of new forms of cyber threats, complicates the process of their detection and analysis. The globalization of information systems creates a threat

from external actors that can negatively affect the information security of the country, which requires the development of effective international protection strategies. Ensuring the security of large volumes of data and their processing in real time is a serious challenge for government agencies, as this requires effective cybersecurity without losing productivity and speed. The constant development of cyber threats, such as adaptive attacks that change according to protection tools, makes it difficult to predict and detect new forms of cybercrime. One of the main elements of this is assessing the effectiveness of antivirus programs that help detect and neutralize malicious programs that threaten the security of systems. Intrusion detection methods are powerful tools for identifying anomalies and abnormal actions in public management systems. Research in this area includes the development of new algorithms and technologies for rapid threat detection and prevention. Multi-layered protection strategies that combine hardware and software solutions are attracting the attention of researchers. Based on the analysis of security in public administration systems, the following recommendations can be offered for data protection and preservation:

1. Raising awareness and training staff – introducing mandatory cybersecurity courses for all employees, which will include regular training, seminars, and online learning.
2. Developing a password policy – establishing strict requirements for password length, complexity, and regular password changes.
3. Systems security audit – conducting regular checks and monitoring network activity to identify anomalies and malfunctions, and eliminate vulnerabilities.
4. Encryption of confidential information – implementing encryption to protect data during transmission and storage, including files and network connections.
5. Protection against unauthorized devices – setting restrictions on access of non-core devices to the network to avoid possible threats from vulnerable connected devices.

6. Using modern antivirus solutions – active use of the latest antivirus programs to effectively detect and block malware.

7. Creating backups – regular backups of important information to restore data in the event of loss or attack.

8. Monitoring and threat detection – setting up monitoring and threat detection systems for rapid response to cyber threats.

International business practice shows that, on the one hand, the use of the above-mentioned technical capabilities of digital platforms is quite widespread, and on the other hand, there are deep intra-country, inter-state and inter-regional differentiations in the ability of economic entities to use them. Let's look at the numbers: in the United States of America, the share of jobs requiring employees with advanced "digital skills" increased from 4.8% in 2002 to 23% in 2016; employment in professions with an average level of "digital intensity" – from 39.5 to 47.5%, against the background of a simultaneous decrease in the share of jobs with a low level of use of digital technologies – from 55.7 to 29.5%, respectively. Today, more than 32 million people in the United States work in "high-digital jobs," 66 million in mid-digital jobs, and 41 million in "low-digital jobs" that require only basic digital skills [19]. According to the results of 2020, the top ten countries in the world in terms of network readiness (out of 134 countries) were: Sweden (with an index of 82.75), Denmark (82.19), Singapore (81.39), the Netherlands (81.37), Switzerland (80.41), Finland (80.16), Norway (79.39), the United States (78.91), Germany (77.48), and the United Kingdom (76.27). However, in the context of economic asymmetries both within and between countries, digital technologies can only exacerbate these inequalities, causing an even greater gap between rich and poor countries. This conclusion is supported by estimates from experts from the Boston Consulting Group, who note that the richest 20% of citizens in high-income countries should spend only a month's salary on the purchase of a basic laptop. At the same time, in middle-income countries, these same 20% of citizens spend six months of their salary,

and in low-income countries – as much as eight months for the same purposes. This confirms the traditional approach to the analysis of the global digital divide, which was formed in the theoretical context of global economic development in the early 2000s. The main idea of this theory is that there is a significant asymmetry between countries that have information resources and those that do not have these resources [19].

Despite the significant difficulties in determining the scale of the digital economy, due to the lack of a single generally accepted definition and the lack of accurate statistical data on its structural components, the system of indicators and metrics for assessing the digital divide remains quite variable, depending on the level of this gap under study. The degree of access of economic entities to the Internet and information and communication technologies is assessed by quantitative parameters, namely, the audience coverage of broadband and mobile Internet (daily, weekly, monthly), the number of subscribers, the speed of the Internet connection and the cost of access to it, the number of households with the Internet, the level of penetration of mobile radiotelephone communication, the average speed of the Internet connection, the types and number of devices for accessing the Internet, etc. The existing deficit of digital skills and literacy is the main factor contributing to the deepening of the digital divide between countries. According to a study by the Boston Consulting Group, more than 60% of the population in low- and middle-income countries lack basic computer skills, such as using copy and paste functions in documents, sending emails with attachments, and transferring files between computers and other devices. At the same time, in high-income countries, almost 60% of youth and adults lack the next level of standard digital skills, such as using basic formulas in spreadsheets, connecting new devices, creating electronic presentations, installing new software, and so on.

The level of the digital divide in the AI component can also be judged by the indicators of patenting innovations in this area:

from the time of the emergence of AI in the 1950s to 2018, about 417 thousand applications for the commercial application of its technologies were filed in the world. At the same time, there are clearly pronounced asymmetries in the structure of patenting of AI methods, in which more than 30% of the total patent portfolio falls on machine learning. At the same time, the most dynamic growth in patent applications over the specified period was recorded in the deep learning segment – 175%, the use of neural networks – 46%; and among the functional applications of AI, the most common today are video analytics (almost half of all patents in the AI sphere), the robotics segment and the development of control methods. In the country distribution of practical use of patent proposals in the field of artificial intelligence, the first place belongs to the USA (39%), followed by the European Union – 19%, China – 19%, India and the Republic of Korea – 6% each, Japan – 4% [19]. The rapid development of digital transformation processes in economic activity stimulates an active response of national governments of different countries, which are increasingly aware of its critical importance for ensuring high competitive positions in the global market. These processes also contribute to optimizing the use of assets by enterprises and business structures, as well as stimulating innovations in national economies and increasing labor efficiency in society. This is confirmed by the fact that recently 32 OECD countries and 6 partners of this group have developed and are actively implementing national digital strategies, programs and projects that fully comply with the digital agenda for Europe, the European Digital Single Market Strategy and the EU Action Plan on e-Government.

Conclusions. Digitalization has a significant impact on the socio-economic security of both European countries and Ukraine. Thanks to the development of digital technologies, new opportunities for economic growth, improved governance and integration with global markets are emerging. However, this process is not without risks, in particular, cybersecurity threats, deepening digital inequality and job

losses in traditional sectors of the economy. In Europe, digitalization is an important component of the economic development strategy, where national digital strategies contribute to increasing the competitiveness and stability of economies. Ukraine, in turn, must actively implement such strategies, develop digital infrastructure and maintain equal access to digital technologies for all segments of the population. Digitalization also improves the efficiency of public administration, but requires significant investments in the development of digital skills of the population and increasing cyber protection. Therefore, to ensure the stability of socio-economic security, it is necessary to take a comprehensive approach to managing digital transformations, taking into account both their opportunities and risks. Overall, digitalization is an important factor in ensuring socio-economic security, but it requires proper regulation and adaptation to the specific needs of each country.

References

1. Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P. Language Models are Few-Shot Learners. Advances in Neural Information Processing Systems (NeurIPS). 2020. URL: https://papers.nips.cc/paper/2020/hash/1457c0d6bfcb4967418bfb8ac142f64a-Abstract.html

2. Khalid, M., & Yousaf, M. M. A Comparative Analysis of Big Data Frameworks: An Adoption Perspective. Applied Sciences, 2021, 11(22), 11033. URL: https://doi.org/10.3390/app112211033

3. Prakash, D. Data-Driven Management: The Impact of Big Data Analytics on Organizational Performance. International Journal for Global Academic & Scientific Research, 2024, 3(2), 12–23. URL: https://journals.icapsr.com/index. php/ijgasr/article/view/74

4. Garcia, C. Reinforcement learning for dynamic pricing and capacity allocation in monetized customer wait-skipping services. Journal of Business Analytics, 2025, 8(1), 36–54. URL: https://doi.org/10.1080/25732 34X.2024.2424542

5. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255–260. URL: https://www.science.org/doi/10.1126/science.aaa8415

6. Oleynikova, L. G., Savenko, D. M., Kolisnyk, K. A. Digitalization of business processes: experience of European countries: section in the monograph. Socio-humanitarian and technical-technological explorations of modern science: collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California: GS Publishing Services, 2023. 226 p. P. 95–100. URL: h ttps://www.eo.kiev.ua/resources/arhivMonographs/Mono_15/Mono_15.pdf

7. Cherep, A. V., Cherep, O. G., Gelman, V. M., Loseva, E. S. European vectors of digitalization of the economy to ensure national security of the state. Publishing house "Young Scientist". No. 11(123), November 2023. URL: https://molodyivchenyi.ua/index.php/journal/article/view/5951

8. Cherep, Alla, Dashko, Iryna, Ohrenych, Julia. Theoretical and methodological bases of formation of the concept of ensuring socio-economic security of enterprises in the context of digitalization of business processes. Baltic Journal of Economic Studies. Volume 10, Number 1. Riga, Latvia: "Baltija Publishing", Vol. 10. No. 1. 2024. 290 pages. P. 237–246. DOI: 10.30525/2256-0742/2024-10-1-237-246. URL: http://www.baltijapublishing.lv/index.php/issue/article/view/2331/2330

9. Cherep, A. V., Dashko, I. M., Ogrenych, Yu. O., Cherep, O. G. Digitalization as a tool for ensuring the quality of educational services, taking into account European experience: collective monograph / edited by A. V. Cherep, I. M. Dashko, Yu. O. Ogrenych, O. G. Cherep. Zaporizhzhia: Publisher FOP Mokshanov V. V., 2024. 300 p. URL: https://dspace.znu.edu.ua/jspui/handle/12345/24081

10. Cherep, A. V., Ogrenych, Yu. O., Oleinikova, L. G., Vasylenko, D. O. Financial market of Ukraine in conditions of digitalization of the economy: current state, problems and prospects: collective monograph "Implementation of the European vector of development of the state economy through digitalization" / edited by A. V. Cherep, I. M. Dashko, Yu. O. Ogrenych, O. G. Cherep, V. M. Gelman. Zaporizhzhia: publisher of FOP Mokshanov V. V., 2024. 290 p. P. 252–263. ISBN 978-617-8064-46-4. DOI: https://doi.org/10.5281/zenodo.14229509

11. Perishko, N. P. The impact of digitalization on the economy: benefits and risks. VSP "Zhytomyr Trade and Economic Vocational College of DTEU", State Educational Institution "Zhytomyr Polytechnic".

https://conf.ztu.edu.ua › uploads No. 12, 2022, WITH. 147–149. URL: https://conf.ztu.edu.ua/wp-content/uploads/2022/12/146.pdf

12. Dovgan, O. I. The concept of digitalization and its use in legislative practice and activities of executive bodies. State Institution "Kharkiv National University of Internal Affairs". 2024. URL: https://www.google.com/search?q=About+https://forumprava.pp.ua/files/121-132-2024-3-FP-Dovhan_13.pdf&tbm=ilp&ctx=atr&sa=X&ved=2ahUKEwiImruMoZ6NAxV8ZvEDHaatH98 Qv5AHegQIABAC

13. Malinovsky, V. Ya. Strategic aspects of digital transformation of the social sphere. Socio-economic problems of the modern period of Ukraine. Lutsk National Technical University, 2021. P. 27–31. URL: https://lib.lntu.edu.ua/sites/default/files/2021-09/Цифровізація.pdf

14. Samoilenko, Alla. Peculiarities of digitalization of the European Union countries in the context of globalization. Bulletin of Economics, no. 1, Mar. 2021, pp. 46–54. DOI: https://doi.org/10.35774/visnyk2021.01.046. URL: https://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1214

15. Shparyk, O. Digital transformation of secondary education: common strategic vectors of the USA and EU countries. Ukrainian Pedagogical Journal, 2022 (3), 33–43. DOI: https://doi.org/10.32405/2411-1317-2022-3-33-43. URL: https://uej.undip.org.ua/index.php/journal/article/view/609

16. Yanenkova, I. G. Factors and ways of developing digitalization in Ukraine. Economy of Ukraine. State Institution "Institute of Economics and Forecasting of the NAS of Ukraine", 2022. No. 3. P. 4–22. URL: http://nbuv.gov.ua/UJRN/EkUk_2022_3_3

17. Goncharenko, I. Cyber threats to the financial sector in times of war. Economy and Society, 2023 (50). DOI: https://doi.org/10.32782/2524-0072/2023-50-82

18. Nagornyak, M. M. Information security in the public administration system: challenges and prospects. No. 1 (2024): Dnipro Scientific Journal of Public Administration, Psychology, Law. DOI: https://doi.org/10.51547/ppp.dp.ua/2024.1.10. URL: https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/567

19. Oliynyk, M. The global problem of digital inequality and its key forms. Economy and Society, 2023 (57). DOI: https://doi.org/10.32782/2524-0072/2023-57-20

MARKOVA Svitlana Viktorivna,
Doctor of Economics, Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID ID: https://orcid.org/0000-0003-0675-0235

CHEREP Oleksandr Grigorovich,
Doctor of Economic Sciences, Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0000-0002-3098-0105

MASLAK Maria Volodymyrivna,
Doctor of Economics, Professor,
National Technical University
"Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-3322-740X

2.2. ADAPTING BUSINESS UNDER MARTIAL LAW WITH THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Introduction. Adaptation of businesses to war conditions using artificial intelligence is becoming extremely relevant in the modern world, as war creates numerous difficulties for enterprises. Damage to infrastructure, limited access to resources, reduction of the workforce – all this threatens the stability and efficiency of business processes. Artificial intelligence, capable of quickly processing large amounts of data and making automated decisions, allows companies to adapt to these conditions. Therefore, scientists in their studies focused on the feasibility and necessity of digitalization in the context of globalization and the use of AI: Alekseeva O. V., Mazur K. V., Kryvogubets V. A. [1], Andros S. V. [2], Harry Bauman, Shahrokh Niku, Francisco J. [3], Hrybinenko O. M. [4], Guralyuk A. G., Kononenko A. G. [5], Guseva O. Yu., Legominova S. V. [6], David Eder, Christoph Buck [7], Oleinikova L. G. [8; 12], Savenko D. M., Kolisnyk K. A. [8], Cherep A. V. [9–12], Cherep O. G. [9; 11], Gelman V. M.,

Loseva E. S. [9], Dashko I. M. [10; 11], Ogrenych Yu. O. [10–12], Vasylenko D. O. [12].

In particular, AI can optimize logistics, predict changes in demand for products and services, and automate key processes, which helps maintain operational efficiency even during crisis situations. Integrating AI into risk management is another important aspect of business adaptation in wartime. AI systems can make predictions and analyze external factors, such as changes in the political and economic arena, which allows businesses to quickly adjust strategies and make more informed decisions. In addition, AI can help with financial management, determine the most optimal ways to reduce costs and ensure the continuity of operations, even when traditional supply channels of goods and services are disrupted. Artificial intelligence also helps maintain business stability in conditions of constant change. In wartime, AI can be used to automate routine tasks, freeing up human resources for more important operations, such as strategic planning or operational management. This helps businesses remain flexible, adapting their processes to a changing environment, ensuring business continuity and reducing the risk of losses associated with unexpected changes or attacks on infrastructure.

Presentation of the main research material. Adaptation of businesses to war conditions using AI is extremely relevant due to the need to quickly respond to constant threats, limited resources and environmental instability. Enterprises are faced with challenges that require new solutions – from maintaining logistics chains to protecting personnel and customers. AI allows you to automate critical processes, analyze large amounts of data in real time, predict risks and ensure flexibility of operations, which is especially important in conditions of military operations and unpredictable changes. In addition, the use of AI creates a competitive advantage for Ukrainian companies in the global market, demonstrating their technological maturity and innovation. In war conditions, AI becomes not only a means of optimizing costs, but also a tool for survival

and growth: from developing military solutions (drones, monitoring systems) to supporting the economy through new products and services. This makes AI not just a technology of the future, but a real resource for national resilience today. The use of AI by Ukrainian enterprises in war conditions is presented in Table 1.

Ukrainian companies are actively implementing AI (Table 1) as a tool for adapting to wartime conditions. For example, the startup Bavovna.AI is developing autonomous drones with GPS-free navigation, and the Zvook project uses AI to detect enemy drones and missiles by sound.

Table 1

Use of AI by Ukrainian enterprises in wartime

Company / Project	The essence of using AI in wartime
Bavovna.AI	Developing autonomous navigation for drones that operate without GPS, using AI to avoid obstacles and counter electronic warfare
Mememe	Using ChatGPT and Midjourney to create a lingerie collection design – automating the creative process in a resource-limited environment
SemanticForce	Social media analysis, fake information detection, public opinion monitoring using neural networks
UA Damage	Automatic recognition of infrastructure damage in satellite images for demining and reconstruction planning
Zvook	AI-based acoustic detection of enemy missiles, drones, and helicopters is used to warn air defenses

Such technologies are critical for defense, security, and rapid response. Meanwhile, civilian companies, such as lingerie brand Meméme, are using generative AI to automate product design, reducing costs and speeding up production. Such examples show that artificial intelligence has become not only a technological advantage, but also a means of survival and business development in times

of crisis. Thanks to AI, companies are able to quickly analyze data, adapt to new challenges, create dual-use products, and actively participate in the reconstruction of the country.

Over the past four years, the field of AI in Ukraine has demonstrated dynamic development (Table 2), despite the challenges caused by the full-scale war. The number of companies working in the field of AI increased from 209 in 2020 to 243 in 2023, which indicates a steady growth of interest in this area. 2021 was especially active, when the number of companies increased by 15 units. In 2023, Ukraine ranked second in terms of the number of AI companies among the countries of Central and Eastern Europe. The number of specialists in the field of AI is also growing. In 2020, there were 3,000 of them, and by 2023 this figure reached 5,200. This growth indicates an increase in interest in the field and the development of relevant educational programs. In particular, in 2023, 106 training programs in artificial intelligence operated in Ukraine, which contributes to the training of new specialists [14]. Investment in the field of AI in Ukraine has fluctuated. In 2020, 22 companies raised $32 million, but by 2023 this amount decreased to $10.8 million, despite an increase in the number of companies to 22. This decrease is associated with the global decline in venture capital investments and the impact of the war on the investment climate. However, in 2023, funding for startups specializing in AI increased by 35% compared to 2022, which indicates the continued interest of investors in this industry [15].

Table 2

Key indicators of AI development in Ukraine for 2020–2023 [4]

Indicator	2020	2021	2022	2023
Number of AI companies	209	224	234	243
Number of AI/ML specialists	3,000	3,800	4,500	5,200
Attracted investments ($ million)	32	25	15.7	10.8
Number of companies with investments	22	20	17	22
Number of educational programs in AI	60	80	95	106

Artificial intelligence (AI) opens up wide opportunities for improving business efficiency in various areas. One of the key areas is the automation of routine operations – from processing documents, invoices, customer requests to managing inventories and logistics. This allows you to reduce personnel costs, speed up work, avoid errors and focus employees' attention on more important strategic tasks. For example, in retail, AI can automatically form orders for suppliers based on sales analytics and demand forecasts. The second important area is data analysis and forecasting. AI is able to study large amounts of information, identify patterns and build accurate forecasts: from consumer behavior to market fluctuations. This helps businesses make informed decisions, reduce risks and respond quickly to changes. For example, banks use AI to assess customer creditworthiness, insurance companies – to detect fraud, and marketing departments – to personalize offers. AI also contributes to innovative business development, creating new products and services. For example, in healthcare, AI is used to develop personalized treatment plans, in agribusiness – to monitor the condition of soils and crops, and in creative industries – to generate content. For Ukrainian companies, especially in wartime, the implementation of AI is not only a way to increase productivity, but also an opportunity to find new niches, attract investments and enter international markets.

Artificial intelligence for business can be classified according to various criteria depending on its functions, purpose and scope. Below is a basic classification of AI for business (Table 3), which helps to understand how and where it can be effectively used:

Analysis of Table 3, which classifies artificial intelligence for business by functional purpose, technology types, and application areas, indicates the wide versatility and practical value of AI in modern conditions. The greatest potential is observed in the areas of analytics and automation, where machine learning and robotic process automation (RPA) significantly reduce time and resource costs. NLP-based communication tools allow companies to serve

Table 3

Classification of AI for business

Category	Usage examples
1. By functional purpose	
Operational AI	Production automation, warehouse management, logistics optimization
Analytical AI	Sales forecasting, market analysis, customer behavior
Communication AI	Chatbots, voice assistants, customer service
Creative AI	Generation of texts, images, designs, videos for advertising
Security AI	Fraud detection, cyber security, access control
2. By type of technology	
Machine Learning	Learns from data and makes decisions – forecasting, recommendations
Natural Language Processing	Human language processing – chatbots, feedback analysis, document management
Computer Vision	Object recognition in photos/videos – quality control, security
Robotic Process Automation (RPA)	Automation of repetitive processes – accounting, bookkeeping
Generative AI	Creating new products – texts, images, music
3. By industry application	
Finances	Credit scoring, fraud detection, automated transaction processing
Trade / e-commerce	Recommendation systems, personalized marketing, demand forecasting
Production	Quality control, predictive maintenance, resource planning
Medicine	Diagnostics, image processing, personalized treatment plans
Agricultural sector	Crop monitoring, crop optimization, drones with computer vision

customers 24/7 without involving additional personnel, which is especially relevant during wartime, when staffing may be limited. In terms of industry application, AI solutions in finance, trade, and medicine are developing most dynamically. Such sectors have a large amount of digital data that can be effectively processed and used for forecasting and decision-making. At the same time, the agricultural sector and manufacturing demonstrate growing interest in computer vision and real-time analytics, which allows optimizing production processes and minimizing losses. Such a comprehensive classification is not only a theoretical, but also a practical basis for the strategic implementation of AI in the business model of enterprises of any scale.

The adaptation of businesses to the conditions of military conflicts using artificial intelligence is taking place not only in Ukraine, but also abroad (Table 4). One of the striking examples is Israeli companies that systematically use AI in the field of defense and civil protection. For example, the startup AnyVision develops facial recognition systems for real-time threat identification, which is actively used in public places during conflicts. The company Windward uses AI to analyze maritime

Table 4

Using AI in war abroad

Country	Company / Project	Scope of AI application	Result / Goal
Israel	AnyVision	Facial recognition, security	Real-time threat detection
Israel	Windward	Maritime transportation, analytics	Detection of illegal activity
Germany	DHL	Logistics, routing	Delivery in closed areas
Great Britain	Darktrace	Cybersecurity	Protection against cyberattacks
Nigeria	Zindi	Humanitarian analytics, supply	Optimization of resources in crisis zones

transportation in order to detect suspicious activity – this is important for the security of logistics in wartime.

In countries supporting Ukraine, AI is helping companies adapt their operations to the new reality. For example, Germany's DHL has implemented intelligent delivery routing systems that automatically adapt to changes in transport infrastructure, roadblocks or closed regions. This has allowed logistics to remain efficient in times of crisis. And the British company Darktrace, which specializes in cybersecurity using AI, protects companies from cyberattacks, including from hostile states. Even in conflict regions of Africa (for example, in Nigeria or Ethiopia), companies are using AI for humanitarian purposes and supporting the economy. In particular, the startup Zindi is helping local businesses use analytics to solve problems with the supply of products or medical resources. This is an example of how intelligent technologies allow businesses to survive and even grow in conditions of instability.

An analysis of Table 5 shows that artificial intelligence is being actively implemented in various countries to adapt businesses to conditions of war or crisis instability. Companies from Israel, Germany, the UK and African countries demonstrate examples of effective use of AI in logistics, security, cybersecurity and resource supply. The most common are solutions that work in real time – such as facial recognition, automatic routing or threat detection. This emphasizes the strategic role of AI in increasing the efficiency and accuracy of decision-making.

On the other hand, the table demonstrates that even in conditions of limited resources, as in Nigeria, AI can become an effective tool for local business. Such examples confirm that technologies are not limited to countries with a high level of development, but are a universal tool for supporting the economy in emergency situations. A common feature of all examples is the focus on continuity of operations and resilience to external threats, which is especially important for Ukrainian companies in the context of war.

Table 5

SWOT analysis of business adaptation to war conditions using AI

S (Strengths) – Strengths	W (Weaknesses) – Weaknesses
Process automation and reduction of the human factor	High initial investment
Rapid analysis of large amounts of data	Insufficient level of digital infrastructure in certain regions
Improving business security and resilience	Lack of qualified IT personnel during the war
Flexibility and scalability of solutions	Possible ethical and legal risks of using AI
O (Opportunities) – Opportunities	**T (Threats) – Threats**
Development of new business models and products	Cyberattacks, data abuse
Entering international markets through innovation	Rapid changes in the regulatory environment
Attracting foreign investment in AI solutions	Dependence on imported software
Cooperation with universities and IT companies	Power outages, internet outages due to fighting

SWOT analysis (Table 5) shows that the use of artificial intelligence to adapt business in wartime has significant strengths – first of all, it is the automation of processes, the ability to quickly analyze large amounts of data and make decisions in real time. Such solutions are especially relevant during times of limited access to personnel, disrupted logistics chains or changes in demand.

Thanks to flexibility and scalability, AI can quickly adapt to new conditions, ensuring the stability and competitiveness of business. At the same time, the analysis shows the presence of significant challenges. The high cost of implementation, dependence on stable infrastructure and the shortage of IT specialists in times of crisis can complicate the use of AI in many regions. Additional threats are cyberattacks and the likelihood of changes in the regulatory

environment. However, taking into account state support, international partnerships and educational and scientific cooperation, most risks can be reduced, opening up new opportunities for sustainable business development even in wartime.

Effective adaptation of businesses to war conditions using artificial intelligence requires not only the technical implementation of digital solutions, but also a strategic vision of management and proper personnel training. Successful integration of AI involves a deep understanding of business needs, the ability to rethink operational processes and the ability to quickly respond to changes in the external environment. The formation of a digital culture in the team is especially important, which involves involving personnel in automation processes, training in new technologies and increasing the overall level of digital literacy.

At the same time, Ukrainian enterprises face a number of challenges, including the high costs of implementing AI solutions, the lack of qualified specialists in this area, as well as ethical risks, in particular those related to data confidentiality and algorithm transparency. These barriers can be overcome through active state support, in particular through tax breaks, grant programs, and stimulating partnerships between businesses and leading IT companies.

With a systematic approach, artificial intelligence can become not only a stabilization tool, but also a powerful factor in the innovative development of Ukrainian business in wartime. The lack of specialists in the field of AI is one of the key problems that hinders the introduction of innovations in the Ukrainian business environment, especially in wartime. Over the past three years, the situation has worsened due to the mass migration of qualified personnel abroad, the mobilization of men of military age, and the destruction of educational infrastructure in a number of regions. Many IT professionals have been forced to change jobs or leave the country, which has led to a decrease in the number of available specialists in high-tech fields, including AI. In addition to the physical outflow

of personnel, there is also a structural problem – a mismatch between market needs and the content of educational programs.

According to think tanks, the demand for data analysts, machine learning specialists, AI engineers, and cybersecurity experts is steadily growing, while domestic universities have only partially adapted their curricula to these challenges.

Even in leading technical universities in Ukraine, specialist training is often theoretical in nature, with a lack of practical work on real AI projects. At the same time, positive developments are already emerging in Ukraine. In 2022–2024, there will be an increase in the number of short-term online programs, bootcamps, and corporate training courses on the basics of AI, which are focused on rapid retraining of personnel. IT companies such as SoftServe, EPAM and Sigma Software are actively investing in the development of internal academies.

However, these initiatives still cover a limited range of individuals. To solve the problem on a systemic scale, government policies are needed to support technical education, in particular, stimulating STEM areas, dual training and integrating AI competencies into broader curricula.

Analysis of the data provided (Table 6) indicates a systematic increase in the demand for specialists in the field of artificial intelligence in Ukraine during 2022–2024. Despite the increase in the number of educational courses and initiatives by IT companies, the real number of qualified AI specialists remains low – in 2024 it was approximately 10,000 people, with a need of at least 33,000. The war significantly exacerbated the problem: migration of specialists, mobilization, reduced investment in education, as well as the lack of coordinated state policy led to an even greater personnel shortage in the industry, which is critically important for the economic stability and technological independence of the country.

A positive trend is the increase in the number of short-term educational programs and the involvement of the private sector

in training personnel. At the same time, this is not enough: most of such courses provide only a basic level of knowledge, and do not train full-fledged AI engineers or researchers [25; 26]. It is obvious that without a comprehensive reform of technical education, modernization of university programs, state stimulation of STEM areas, and creation of a national strategy for the development of artificial intelligence, it will be impossible to bridge the gap between demand and supply. Such a strategy should become part of a broader policy of digital transformation of Ukraine in the context of war and post-war recovery.

Table 6

Estimated number of AI specialists in Ukraine over the last 3 years (taking into account the overall IT market, research and practice) [17]

Year	Number of AI specialists in Ukraine	Assessment of staff shortages	Comment
2022	~7,000	~15,000	Many specialists went abroad or were mobilized. The market shrank
2023	~8,500	~20,000	Demand is growing faster than new staff are being trained. Education is not keeping up
2024	~10,000	~23,000	The number of courses and programs is growing, but there is still a significant gap between demand and supply

As a result of the full-scale Russian invasion and the economic and social consequences of the war, the population of Ukraine has decreased significantly. Over the past three years, the country's population has decreased by approximately 10 million people. As of 2025, the total population is about 38.6 million people, of whom approximately 25–28 million remain in Ukraine, while the rest have left or are internally displaced persons (Table 7). In the first year

of the war alone, the number of refugees from Ukraine exceeded 6 million, which significantly affected the economic and social situation in the country. Migration processes have become one of the greatest challenges for Ukraine's post-war recovery.

Most refugees have left for European countries such as Poland, Germany and the Czech Republic, where they seek protection and jobs. Internal migration also remains high, with approximately 3.7 million people displaced within Ukraine. These changes, particularly in the composition of the labor force, may have long-term economic consequences, requiring not only humanitarian but also economic adaptation to maintain production capacity [23].

Table 7

Population of Ukraine and migration (2022–2025) [18; 19; 20]

Indicator	2022	2023	2024	2025 (estimate)
Total population	~40.7 million people	~39.2 million people	~38.6 million people	~38.6 million people
Migration (refugees abroad)	~6.5 million people	~6.8 million people	~6.9 million people	~7.0 million people
Internally displaced persons	~7.0 million people	~6.3 million people	~3.7 million people	~3.7 million people
Population under Ukrainian control	~28.0 million people	~27.5 million people	~25.0–27.0 million people	~25.0–28.0 million people

As of 2023, there are about 307,600 IT professionals in Ukraine, of which 238,000 work directly in the country, and the rest abroad (Table 8). This is approximately 0.8% of the total population of Ukraine, which is estimated at 38.6 million people. Globally, according to 2022 data, the number of professional programmers

is 26.9 million people, which is equivalent to 0.3% of the total world population, which exceeds 8 billion people.

Table 8

Share of IT professionals in the total population

Country / Region	Number of IT specialists	Total population	Share of IT professionals
Ukraine	307600	38600000	0.8%
World	26900000	8000000000	0.3%

The data in Table 6 shows that in Ukraine the share of IT specialists is significantly higher than the world average, which emphasizes the importance of this industry for the national economy and technological development. As of 2025, China is the leader in the number of IT specialists in the world, with 7 million programmers. This is due to the high level of investment in technological infrastructure, the active development of startups and state support in the field of artificial intelligence and digital technologies. Chinese cities such as Shenzhen, Beijing and Shanghai have become important centers for software developers. India ranks second with 5.8 million programmers. The country is known for its strong STEM education system and a significant number of graduates in technical specialties. Cities such as Bangalore, Hyderabad and Chennai are important hubs for software development and outsourcing services. According to forecasts, India could become the largest market for AI services by 2027, in particular thanks to initiatives such as the “IndiaAI Mission” [22].

The data in Table 9 indicate that China and India not only lead in the number of IT specialists, but also actively invest in the development of technology industries, which contributes to their further growth on the global stage.

Ukraine is actively investing in the development of technology industries, despite the difficult conditions of the war. In 2024,

investments in the technology sector increased by 120%, reaching $147 million, of which 32% were directed to the early stages of project development. This indicates a high interest in innovations and startups, even in war conditions [26]. Ukraine's technology sector continues to demonstrate resilience and potential for growth. In 2023, exports of IT services amounted to $6.7 billion, which is about 5% of the country's GDP. This confirms the importance of the technology industry for the Ukrainian economy and its ability to attract investments even in difficult conditions. Ukraine is demonstrating significant progress in the development of technology industries, despite the difficult conditions of the war. In 2024, investments in the technology sector increased by 120%, reaching $147 million. In particular, 32% of these investments were directed to the early stages of project development, which indicates a high interest in innovations and startups. Among the largest deals of the year are investments in the British fintech company Carmoola and the Jome platform, which simplifies the process of buying a home. These data confirm the resilience and potential of the Ukrainian technology sector

Table 9

Number of IT professionals by country (2025)

Country	Number of programmers
China	7000000
India	5800000
USA	4400000
Japan	1200000
Brazil	500000
Singapore	200000
Australia	100000
Mexico	100000
Colombia	80000
Hungary	80000

even in wartime conditions [26]. Exports of IT services also continue to be an important source of foreign exchange earnings. In 2024, exports of IT services amounted to $6.45 billion, which is about 3.5% of the country's GDP. Despite a 25% drop in export volumes compared to 2021, the IT sector remains the second largest export sector after agriculture. The main sales markets are the USA, the UK and Malta. This indicates the importance of the IT industry for the Ukrainian economy and its ability to adapt to new conditions.

To improve development and investment in Ukraine's IT industry, we should focus on several key aspects:

1. Improving education and skills. Investment in education is critical for the development of the IT sector. Since skills directly affect innovation and productivity, Ukraine needs to improve training programs for future IT professionals, providing more opportunities for internships, practical courses and certifications. This will contribute to the formation of a highly skilled workforce capable of working with advanced technologies such as artificial intelligence, blockchain and the Internet of Things.

2. Support for startups and innovative projects. Creating favorable conditions for the development of startups can stimulate investment in new technologies. Ukraine needs to develop infrastructure to support startups, create investment funds specializing in financing technological innovations. It is also important to provide tax benefits for companies engaged in research and innovation, and develop partnerships with international investors.

3. Development of state support and regulations. It is necessary to strengthen the role of the state in supporting technology industries through the adoption of new legislative initiatives that stimulate investments in the IT sphere. It is important to reduce bureaucratic barriers, ensure the protection of intellectual property and simplify procedures for investors. The development of programs that support technology companies through grants and subsidies will also become an important factor in attracting investment.

4. International cooperation and attracting foreign investment. Deepening cooperation with international partners in the field of technology can provide new opportunities for Ukrainian IT companies. Ukraine can advantageously position itself in the international market through participation in global IT initiatives, such as startup platforms or development programs within the framework of the European Union and other international organizations.

Through strategic development in these areas, Ukraine has the potential to become one of the leading hubs for technological innovation in Eastern Europe, which will attract significant investments and create new opportunities for economic growth.

Improving the level of education and skills of personnel in Ukraine is one of the main factors contributing to the development of the IT industry and ensuring its competitiveness in the global market. In the context of rapid technological changes, it is important to constantly update curricula, focusing them on the modern needs of the industry. This includes not only theoretical knowledge, but also practical skills in areas such as artificial intelligence, machine learning, software development, cybersecurity and big data.

The active implementation of training programs through online courses, internships and certification programs allows students and young professionals to adapt faster to the changing technological environment. In addition, it is necessary to focus on developing cooperation between educational institutions and IT companies to create a system of continuous education and professional development. This will expand opportunities for students to gain real work experience while studying, and will also contribute to the formation of a talent pool ready to work in conditions of high competition in the global market.

An important aspect is also increasing digital literacy among different segments of the population, as IT competencies are becoming important not only for specialists in the industry, but also for most workers in other fields.

These steps can significantly improve the level of education and skills in Ukraine, contributing to the development of highly qualified personnel for the IT sector and other sectors of the economy (Fig. 1).

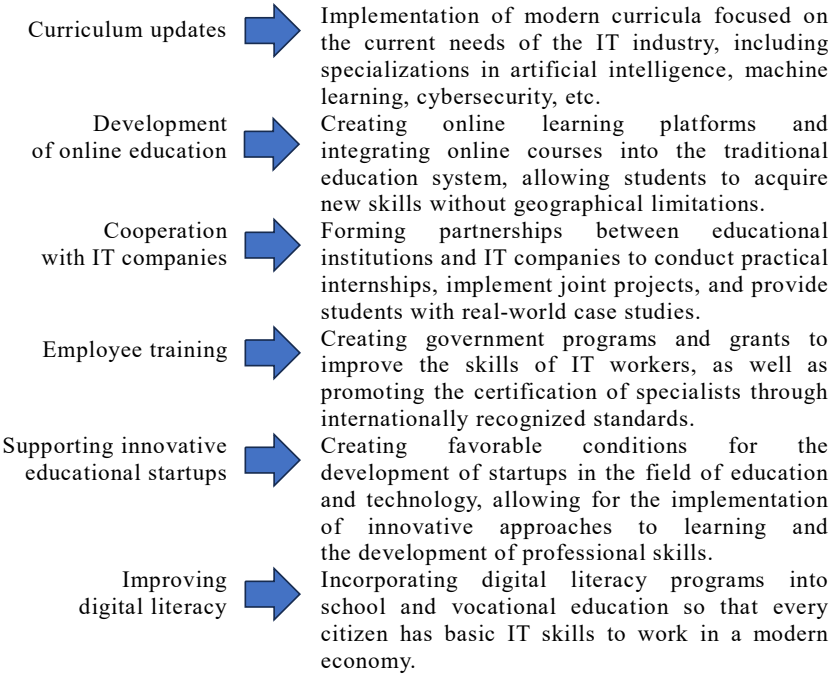

Fig. 1. Key steps of the state to improve the level of education and qualifications in Ukraine

Source: compiled by the authors

As of 2024, there are over 300 higher education institutions operating in Ukraine that train specialists in various fields, including information technologies. According to the Ministry of Education and Science of Ukraine, in 2023 the number of students in IT-related specialties exceeded 100 thousand people. This indicates a high demand for IT education and a growing interest in this area among young people. However, despite the significant number of educational

institutions and students, there is a need to improve educational programs and improve the quality of specialist training.

In particular, it is necessary to update curricula, integrate practical internships, cooperate with IT companies, and implement international education standards. This will ensure that the training of specialists meets the requirements of the modern labor market and contribute to the development of the IT industry in Ukraine.

The universities listed in Table 10 are leaders in Ukraine in terms of the number of students in the field of information technology and offer competitive study programs. In particular, Kyiv Polytechnic Institute and Taras Shevchenko National University of Kyiv have the highest tuition fees, which may indicate a high level of educational services and infrastructure. While Sumy State University offers more affordable prices, which may be attractive to students with limited financial resources.

Table 10

Leading universities of Ukraine that train specialists in the field of information technologies [27–30]

University name	Number of students	Tuition fee (UAH/year)	IT specialties
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"	~21,000	43,900–54,900	Computer Science, Software Engineering, Cybersecurity
Taras Shevchenko National University of Kyiv	~26,000	50,900–66,600	Computer Science, Psychology, Management
Lviv Polytechnic National University	~33,500	36,800–46,200	Computer Science, Cybersecurity
V. N. Karazin Kharkiv National University	~20,000	23,000–31,000	Computer Science, Management
Sumy State University	~15,000	13,440–37,000	Computer Science, Management

In Ukraine, the ecosystem of EdTech startups has been actively developing in recent years, in particular due to the cooperation of private business, the state and public organizations. Accelerators (for example, Ukrainian Startup Fund, Unit.City, 1991 Open Data Incubator) play an important role in supporting educational startups, providing funding, mentoring support and the opportunity to pilot launch educational products. Individual projects, such as Prometheus, EdEra and GIOS, have become an example of the successful implementation of innovative ideas in education – from online courses to interactive mathematics platforms focused on the Ukrainian market. In addition, after the start of a full-scale war in 2022, the demand for innovative educational solutions increased, which stimulated the launch of new initiatives aimed at distance learning, mental health of students, adaptation of displaced persons and support for teachers. Thus, the Ministry of Education and Science of Ukraine, together with partners (USAID, UNICEF, Google) initiated projects on the digitalization of education and grant support for startups. This experience demonstrates the potential of the Ukrainian EdTech sector as an important component of the national innovation economy.

StudyDive is a Ukrainian platform for corporate online learning that actively integrates artificial intelligence to personalize the educational process. The service analyzes the needs of company employees, their learning dynamics, interests, and course completion results, after which the AI module generates individual recommendations for the next topics or courses. This allows employees to develop precisely those competencies that correspond to their position and career track. Companies that have implemented StudyDive note an increase in staff engagement in learning and an increase in training effectiveness. The project received funding from the Ukrainian Startup Fund and a number of private investors. It is used by both Ukrainian and international companies, in particular in the IT, finance, and logistics industries. The use of AI has allowed to reduce training costs by up to 30%, optimize HR processes, and make the educational

trajectory of each employee more effective. StudyDive is an example of how innovative solutions can improve professional education and the internal culture of continuous learning in a business environment.

Despite its successes, StudyDive also faced a number of difficulties in the process of implementing artificial intelligence into the corporate training system. One of the main problems was the lack of understanding of AI solutions among customers – some companies expected instant results from process automation, without taking into account the need for preliminary data analysis and content adaptation. In addition, the AI module did not always correctly determine the educational needs of employees in narrowly specialized fields, which led to recommendations of irrelevant courses. Another challenge was the integration of StudyDive into the internal HR systems of enterprises, especially state-owned ones or those with outdated IT infrastructure. There were also complaints from users about the excessive "machinery" of recommendations that did not take into account the individual context or motivation of the employee. These difficulties forced the StudyDive team to invest more time in tuning the algorithms, testing in different markets, and additional training of customers on the correct use of the platform. Thus, even innovative AI products require a flexible approach and constant refinement to achieve a sustainable effect [31].

Adapting businesses to wartime conditions requires rapid transformation not only in terms of technology, but also in the level of digital literacy of employees. Today, artificial intelligence is an important tool that allows enterprises to respond more quickly to market changes and adapt their strategies to new conditions. However, for the effective use of such technologies, it is necessary for employees to have basic and advanced knowledge in the field of digital technologies. In this context, the development of digital literacy is important, which will provide employees with the ability to use AI to automate processes, analyze data and make decisions in real time.

Digital literacy encompasses more than just the ability to work with computer programs or use online resources. It includes the ability

to effectively interact with intelligent systems that process large amounts of data, predict business trends, and optimize processes in real time. In wartime, when information may be limited and access to traditional resources is difficult, a business's ability to adapt quickly through the use of AI becomes a key success factor. Improving digital literacy at all levels of the organization allows a business to remain competitive even in the most challenging conditions. Integrating AI into business processes cannot be effective without the proper level of training. This includes both basic skills in working with new digital tools and the ability to use more complex systems, such as workflow automation or a forecasting system. Therefore, for a business to adapt to wartime conditions to be successful, it is important not only to purchase new technologies, but also to invest in education and training for personnel. Legislative initiatives and documents in Ukraine that contribute to the activation of digital literacy and its development in business, in particular in war conditions, are identified in Table 11. These legislative initiatives contribute to the development of digital literacy among citizens and businesses, which is an important factor in adapting to the rapidly changing conditions of war, in particular through the integration of artificial intelligence into work processes.

Table 11

Legislative initiatives and documents in Ukraine that contribute to the activation of digital literacy and its development in business [32–37]

Name of law/ initiative	Description	Digital literacy
1	2	3
Law of Ukraine "On Electronic Communications"	The law regulating electronic communications in Ukraine, ensuring the availability and quality of digital services	Promotes the development of digital skills for using electronic services and resources

Table 11 (continued)

1	2	3
Law of Ukraine "On Stimulating the Development of the Digital Economy"	A law supporting the development of the digital economy through legal initiatives and funding	Defines the foundations for the development of digital skills and educational programs for businesses in the field of digital technologies
Resolution of the Cabinet of Ministers of Ukraine "On Open Data"	A regulation defining a set of data to be made public as open data, facilitating access to information	Enhances skills in analyzing and using open data to increase digital literacy in business
Decision of the National Security and Defense Council of Ukraine "Cybersecurity Strategy"	A strategy that defines the main priorities for ensuring cybersecurity in Ukraine	Covers the development of digital literacy to ensure data security and information protection in digital environments
Resolution of the Cabinet of Ministers of Ukraine "Ministry of Digital Transformation"	A resolution that defines the functioning of the Ministry of Digital Transformation to implement state policy	Promotes the development of digital literacy through the implementation of state programs for the digitalization of society
Resolution of the Cabinet of Ministers of Ukraine "Digital Development Strategy"	Ordinance approving the strategy for the development of digital technologies and innovation activities for the period until 2030	Supports initiatives that develop digital skills among citizens and employees through educational programs

The conditions of martial law in Ukraine have forced businesses to look for new tools for survival, rapid restructuring, and effective adaptation to an unstable environment. One of such solutions has been the active implementation of artificial intelligence (AI) technologies, which today act not only as an innovative but also as a strategic resource in crisis conditions. AI allows businesses to optimize internal processes, reduce costs, predict risks, support customers online, and ensure business continuity even with limited resources or the physical presence of employees. The implementation of digital transformations in business is directly related to the level of digital literacy of employees. The legislative framework of Ukraine already creates favorable conditions for the development of digital competencies – in particular, through the support of open data, the development of electronic communications, the implementation of the digital economy, and cybersecurity. Programs launched by the Ministry of Digital Transformation contribute to the formation of educational opportunities for entrepreneurs and employees, which increases the readiness of businesses to integrate intelligent systems.

The positive experience of domestic startups, such as StudyDive and other AI projects, demonstrates the real benefits and prospects of AI in difficult economic conditions. At the same time, there are also challenges – related to the imperfection of the infrastructure, the risks of cyberattacks, and insufficient qualifications of personnel. However, systemic state support for digital transformation, the growth of interest in innovative business models, and the need for new formats of work contribute to the fact that AI is becoming a key element of the adaptation strategy of Ukrainian business during the war. In addition to the adaptation function, artificial intelligence during the war period also plays the role of a driver of innovative business strategy. Companies that quickly integrated AI solutions – in particular, chatbots for customer support, automated logistics analysis systems, marketing analytics, and demand forecasting – were able not only to survive, but also to expand sales markets, switch to a remote work

format, and create new values for consumers. AI is also actively used in the fields of security, financial technology, insurance, agribusiness, and education, where it helps compensate for the lack of human resources and respond quickly to changes.

At the same time, the further development of AI in Ukrainian business requires targeted investments in human capital, modernization of educational programs and support for the startup ecosystem. An important role is played by state policy in the field of digitalization, in particular, the implementation of the Digital Development Strategy, support for national EdTech platforms, and digital literacy of employees and managers. The conditions of war have reinforced the understanding that digital technologies and AI are not a luxury, but a critically important tool for the sustainability, mobility and competitiveness of business in the 21st century.

Conclusions. The state plays a key role in creating a favorable environment for the digital transformation of business, especially in conditions of martial law. Through the activities of the Ministry of Digital Transformation, national programs are implemented that are aimed at increasing the digital literacy of citizens, developing e-government and stimulating innovative activity. In particular, the platform "Diya.Digital Education" provides free access to educational courses that help entrepreneurs and employees master basic and specialized digital skills. In addition, the state initiates partnership projects with international organizations, thanks to which Ukrainian business gains access to mentoring, financing and technical support in the field of artificial intelligence. A number of important documents have already been adopted at the legislative level, in particular the Digital Development Strategy, the Law "On Stimulating the Development of the Digital Economy", as well as regulatory acts on cybersecurity and open data. Such solutions form a holistic infrastructure for the digital transformation of business, including data protection, ensuring legal regulation of AI technologies and supporting startups. In times of war, it is government

support – in the form of grants, tax breaks, and innovation incubators – that becomes critically important for the survival and development of enterprises seeking to implement intelligent technologies and remain competitive in domestic and international markets.

References

1. Alekseeva, O. V., Mazur, K. V., Kryvogubets, V. A. Digitalization as an important factor in the formation of the competitiveness of agricultural enterprises. Problems of modern transformations. Series: economics and management. 2024. No. 12. DOI: https://doi.org/10.54929/2786-5738-2024-12-04-06

2. Andros, S. V. Digitalization and enterprises: new trends in innovative development. Economic Journal of Odessa Polytechnic University. 2019. No. 4(10). P. 5–13. URL: https://economics.opu.ua/ejopu/2019/No4/5.pdf. DOI: 10.5281/zenodo.3757950

3. Harry, Bouwman, Shahrokh, Nikou, Francisco, J. Molina-Castillo, Mark de Reuver [1], The impact of digitalization on business models. Digital Policy, Regulation and Governance. 2018. Vol. 20. No. 2. R. 105–124. DOI: 10.1108/DPRG-07-2017-0039

4. Hrybinenko, O. M. Digitalization of the economy in the new paradigm of digital transformation. International relations. Series. Economic sciences. 2018. No. 16. URL: http://journals.iir.kiev.ua/index.php/ec_n/article/view/3523/3197

5. Guralyuk, A. G., Kononenko, A. G. [1], Peculiarities of training modern specialists in the conditions of an open educational environment of higher education institutions. Innovative Pedagogy. 2022. Issue 51, vol. 1. Pp. 9–13. DOI: https://doi. org/10.32782/2663-6085/2022/51.1.1

6. Guseva, O. Yu., Legominova, S. V. Digitalization – as a tool for improving business processes, their optimization. Economics. Management. Business. 2018, No. 1(23). P. 33–39. URL: http://nbuv.gov.ua/UJRN/ecmebi_2018_1_7

7. David, Eder, Christoph, Buck. The Impact of Digitization on Business Models – A Systematic Literature Review. Research Center Finance and Information Management. 24 Americas Conference on Information Systems, New Orleans, August 2018. P. 2–10.

8. Oleynikova, L. G., Savenko, D. M., Kolisnyk, K. A. Digitalization of business processes: experience of European countries: section in the monograph. Socio-humanitarian and technical-technological explorations of modern science: collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California: GS Publishing Services, 2023. 226 p. P. 95–100. URL: https://www.eo.kiev.ua/resources/arhivMonographs/Mono_15/Mono_15.pdf

9. Cherep, A. V., Cherep, O. G., Gelman, V. M., Loseva, E. S. European vectors of digitalization of the economy to ensure national security of the state. Publishing house "Young Scientist" No. 11(123) November 2023. URL: https://molodyivchenyi.ua/index.php/journal/article/view/5951

10. Cherep, Alla, Dashko, Iryna, Ohrenych, Yulia. Theoretical and methodological bases of formation of the concept of ensuring socio-economic security of enterprises in the context of digitalization of business processes. Baltic Journal of Economic Studies. Volume 10. Number 1. Riga, Latvia: "Baltija Publishing", 2024. Vol. 10. No. 1. 290 pages. P. 237–246. DOI: 10.30525/2256-0742/2024-10-1-237-246. URL: http://www.baltijapublishing.lv/index.php/issue/article/view/2331/2330

11. Cherep, A. V., Dashko, I. M., Ogrenych, Yu. O., Cherep, O. G. Digitalization as a tool for ensuring the quality of educational services taking into account European experience: collective monograph / ed. A. V. Cherep, I. M. Dashko, Yu. O. Ogrenych, O. G. Cherep. Zaporizhzhia: Publisher FOP Mokshanov V. V., 2024. 300 p. URL: https://dspace.znu.edu.ua/jspui/handle/12345/24081

12. Cherep, A. V., Ogrenych, Yu. O., Oleinikova, L. G., Vasylenko, D. O. Financial market of Ukraine in conditions of digitalization of the economy: current state, problems and prospects: collective monograph "Implementation of the European vector of development of the state economy through digitalization" / edited by A. V. Cherep, I. M. Dashko, Yu. O. Ogrenych, O. G. Cherep, V. M. Gelman. Zaporizhzhia: publisher of FOP Mokshanov V. V., 2024. 290 p. P. 252–263. ISBN 978-617-8064-46-4. DOI: https://doi.org/10.5281/zenodo.14229509

13. Ukraine ranks second in the number of AI companies in Central and Eastern Europe: results of a study on artificial intelligence. Ministry of Digital Transformation. URL: https://thedigital.gov.ua/news/ukraina-

posidae-druge-mistse-za-kilkistyu-shi-kompaniy-u-tsentralniy-ta-skhidniy-evropi-rezultati-doslidzhennya-pro-shtuchniy-intelekt?utm_source=chatgpt.com (date of application: 05.05.2025).

14. The Ministry of Digital Affairs expects the number of artificial intelligence specialists to grow by 330% – Economic Truth. URL: https://epravda.com.ua/news/2024/06/19/715429/?utm_source=chatgpt.com (date of application: 05.05.2025).

15. Artificial Intelligence: Data for 2015–2023. URL: https://skilky-skilky.info/za-kilkistiu-shi-kompaniy-ukraina-zaymaie-2-mistse-u-tsentralno-skhidniy-yevropi/?utm_source=chatgpt.com (date of application: 05.05.2025).

16. Artificial intelligence in Ukraine – how it works, which companies use it and what salaries. URL: https://24tv.ua/shtuchniy-intelekt-ukrayini-de-navchitisya-yaki-zarplati-yaki_n2579641?utm_source=chatgpt.com (date of application: 05.05.2025).

17. Home – IT Ukraine Association. URL: https://itukraine.org.ua/ (date of application: 05.05.2025).

18. Situation Ukraine Refugee Situation. URL: https://data.unhcr.org/en/situations/ukraine (date of application: 05.05.2025).

19. Ukraine is one of the leaders in brain drain from the country. Ukrinform. 2024. URL: https://www.ukrinform.ua/rubric-society/3850351-ukraina-e-odnim-iz-lideriv-vidtoku-mizkiv-iz kraini-ekspertka.html (date of application: 05.05.2025).

20. Fleeing war or leaving deliberately. How migration from Ukraine has changed and what will be its consequences. BBC. 2024. URL: https://www.bbc.com/ukrainian/articles/c93px84133jo (date of application: 05.05.2025).

21. Forced Migration and War in Ukraine. Cedos. 2022. URL: https://cedos.org.ua/researches/vymushena-migracziya-i-vijna-v-ukrayini-24-bereznya-10-chervnya 2022/ (date of application: 05.05.2025).

22. Ambani's Reliance Industries Solidifies India in Global AI RaceE. URL: https://time.com/7018294/india-ai-artificial-intelligence-ambani/?utm_source= chatgpt.com (date of application: 05.05.2025).

23. Dashko, I., Cherep, O., Mykhailichenko, L. Formation of labor supply at Ukrainian enterprises in the war and post-war periods. Bulletin

of the Khmelnytsky National University. 2023, No. 5. P. 57–64 (access date: 05.05.2025).

24. Cherep, A. V., Voronkova, V. G., Cherep, O. G. The concept of blockchain economy as a new type of economy in the conditions of digitalization: a chapter in the monograph "Modern scientific strategies of development". Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California: GS Publishing. Services, 2022. P. 54–62. URL: https://www.eo.kiev.ua/resources/arhivMonographs/mono2022_dev_008.pdf (date of application: 05.05.2025).

25. Voronkova, V. G., Cherep, A. V., Cherep, O. G. Development of the network (internet economy) in the context of digitalization: principles, laws, development trends. "Science and society: trends of interaction": collective monograph / Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California: GS Publishing Services, 2023. 271 p. P. 31–48. URL: https://www.eo.kiev.ua/resources/arhivMonographs/mono_2023_12.pdf (date of application: 05.05.2025).

26. Investments in the technology sector in Ukraine will increase by 120% in 2024. URL: https://en.interfax.com.ua/news/investments/1053010.html?utm_source=chatgpt.com (date of application: 05.05.2025).

27. Official website of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". URL: https://kpi.ua/ (date of application: 05.05.2025).

28. Official website of Taras Shevchenko National University of Kyiv. URL: https://knu.ua/ (date of application: 05.05.2025).

29. Official website of the Lviv Polytechnic National University. URL: https://lpnu.ua/ (date of application: 05.05.2025).

30. Official website of V. N. Karazin Kharkiv National University. URL: https://karazin.ua/ (date of application: 05.05.2025).

31. Ukrainian Startup Fun (application date: 05.05.2025). d – Innovation Development Fund. URL: https://usf.com.ua/ (date of application: 05.05.2025).

32. Law of Ukraine "On Electronic Communications". URL: https://zakon.rada.gov.ua/go/1089-20 (date of application: 05.05.2025).

33. Law of Ukraine "On Stimulating the Development of the Digital Economy in Ukraine". URL: https://zakon.rada.gov.ua/go/1667-20 (date of application: 05.05.2025).

34. Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Regulation on Data Sets Subject to Publication in the Form of Open Data". URL: https://zakon.rada.gov.ua/go/835-2015-п (date of application: 05.05.2025).

35. Decision of the National Security and Defense Council of Ukraine "On Approval of the Cybersecurity Strategy of Ukraine". URL: https://zakon.rada.gov.ua/go/447/2021 (date of application: 05.05.2025).

36. Resolution of the Cabinet of Ministers of Ukraine "Issues of the Ministry of Digital Transformation". URL: https://zakon.rada.gov.ua/go/856-2019-п (date of application: 05.05.2025).

37. Order of the Cabinet of Ministers of Ukraine "On Approval of the Strategy for Digital Development of Innovative Activity of Ukraine for the Period Until 2030". URL: https://zakon.rada.gov.ua/go/1351-2024-p (date of application: 05.05.2025).

CHEREP Oleksandr Grigorovich,
Doctor of Economic Sciences, Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID: http://orcid.org/0000-0002-3098-0105

2.3. DIGITALIZATION AS A NECESSARY CONDITION FOR BUSINESS DEVELOPMENT IN UKRAINE

Introduction. Small and medium-sized enterprises (SMEs) play an important role in a market economy, being its main element. They contribute to the stability of the country's economy, replenish the budget, provide employment, supply goods and services to the market, and create a competitive environment. SMEs demonstrate flexibility in rapidly changing social conditions, quickly adapt to market changes and introduce modern technologies. The development of SMEs helps to form the middle class, strengthen civil society, reduce social inequality and tension, accelerate the democratization of market relations and ensure social stability.

At the same time, SMEs are very vulnerable to economic conditions, reacting quickly to any changes or crises. Because of this, they often have to overcome significant difficulties that hinder their development and success. The war has affected all aspects of SMEs' activities, including finance, production, logistics, communications, information systems, innovation and organization. Entrepreneurs face the devastating consequences of war and, in a situation of uncertainty, are forced to confront numerous risks and challenges in order to maintain, restore and develop their production potential and protect jobs.

The state and the EU see business digitalization as one of the priority areas for improving the stagnation of small and medium-sized businesses. In this article, I will examine the strengths and weaknesses of the digital transformation of SMEs, as well as the opportunities and threats of the digital transformation of small and medium-sized businesses in wartime.

Presentation of the main material. Digitalization is the process of integrating electronic and digital devices, systems, and tools into the physical world, establishing their interaction through electronic communications. This creates conditions for combining virtual and physical environments, forming the so-called cyber-physical space.

Digitalization as a social phenomenon became widespread in the 1960s and 1970s. It can be characterized by three main features:

1. Converting all types of content from analog, physical, and static formats to digital, making it mobile and personalized. This allows people to manage their content, send information requests, and create a personalized way of working with information.
2. The transition to simplified communication technologies, where technology acts only as a tool for communication, and its key feature becomes ease of management.
3. Transformation of communications into heterogeneous: vertical, hierarchical models lose their significance, giving way to a network structure of information exchange [1].

Among the strengths of SME digital transformation are:

1. Simplification of financial transactions, increasing the role of electronic and digital money. For example, legal entities can make payments and receive other banking services at any time of the day and without days off, while not paying anything for transactions during "after-hours" hours. Online banking allows you to make payments remotely and spend a minimum of time. Bank services have become more accessible and extensive.

2. Developing remote work capabilities. During the 2020 pandemic, entrepreneurs were forced to transform the way they managed their teams overnight. In an emergency, entire departments were moved to remote work. This meant that normal processes were only available online. The pandemic, and then the war, showed that SMEs had to go digital to keep up with the changing business environment.

3. Implementation of an electronic document management system. Thanks to digitalization, it is possible to improve business processes, reduce costs for daily operations, optimize the staff and increase work efficiency. For example, this is manifested in expanding the number and improving the quality of electronic government services available on the Unified State Ukrainian Web Portal of Electronic Services:

– through the use of the Diya Portal mobile application (Diya), with a special emphasis on services for micro and small enterprises, ensuring regular and high-quality feedback;

– interaction with counterparties – Vchasno portal – electronic B2B document flow;

– optimization of internal accounting processes of SMEs – BAS software products and their analogues (note – since 2020, BAS products have been under sanctions, but overall they have a market share of applied software for SMEs of 25%).

In Ukraine, there is such a structure as the "Union of Business Automatizers", which includes companies specializing in creating digital solutions to solve various business problems. They also provide

services for the implementation and support of information systems for management and accounting. The relevance of digital transformation is confirmed by the growing number of implemented automated systems in Ukraine, which is schematically shown. The analysis covers the period from 2005 to June 2024 [2].

4. Increasing market accessibility and openness. Digitalization empowers SMEs to compete more effectively, offering tools to expand market presence, reduce costs and improve service quality. Consumers are increasingly choosing online shopping and digital services. SMEs that adopt digital technologies better understand customer preferences and can quickly adapt to changing customer needs.

5. Productivity growth. Over the past two decades, the digital economy has experienced rapid growth thanks to a series of significant technological breakthroughs. In particular, the emergence of Web 2.0 transformed the Internet into an interactive space where users not only consume information, but also create and share content. The popularity of social networks, video platforms, and blogs has opened up new horizons for communication, commerce, and self-expression. At the same time, the rapid development of e-commerce has become an important factor in the flourishing of the digital economy. Companies have quickly adapted to the possibilities of online sales, providing consumers with convenient access to goods and services. Global e-commerce leaders such as Amazon, Alibaba, and eBay have significantly changed the way products are consumed and distributed [3]. Digital technologies have also contributed to the introduction of more flexible and adaptive production systems. Enterprise resource planning (ERP) software and resource planning systems help companies better coordinate operations, optimize inventory, and respond quickly to changes in demand. This flexibility allows companies to adapt more quickly to market conditions and offer products and services that better meet customer expectations [4].

6. Lowering the cost of goods and services. The use of innovative technologies such as cloud computing, big data analytics, and

e-commerce provides SMEs with opportunities to introduce new products and services at lower cost. Digital technologies have also improved collaboration and interaction in global supply chains. Through e-commerce platforms, professional social networks, and online communication tools, companies have gained the ability to share data in real time with suppliers, partners, and customers around the world. This has increased transparency and openness in supply chains, and has helped reduce delays, errors, and inefficiencies [5].

7. Reducing bureaucracy. Online services make it more accessible for SMEs.

Although digital technologies are now widespread, their weaknesses have not been sufficiently studied. Among these weaknesses is the vulnerability of digital systems to hacking, which can lead to unauthorized access to personal data. The amount of data collected by Internet of Things sensors is constantly growing, raising concerns about privacy violations. The main problem is the lack of full consent for the collection and processing of personal data, as well as uncertainty about what data should be collected and how to analyze it. This creates a risk of loss of privacy.

The Ukrainian Center for Minds conducted a survey of 145 experts who outlined the most common weaknesses in enterprise digitalization in Ukraine [6].

Digitalization brings the greatest benefits to trading companies and banks. “Disruptive technologies” (such as robotics, blockchain, neural networks, artificial intelligence, quantum technologies, virtual and augmented reality) contribute to the optimization of production processes, automation, remote control, which, however, can lead to the reduction or complete disappearance of jobs.

To summarize, the key disadvantages of digitalization for SMEs include:

– giving the state the leverage to manage SMEs and depriving them of autonomy;

– the advantage of multinational corporations in implementing digitalization over SMEs due to the availability of greater resources (financial, human, etc.);

– dependence on companies providing information and communication services and digital technologies.

At the same time, concerns about the risks of digitalization have increased significantly in recent times. Many companies are afraid of technological innovations, in particular, possible cyber threats.

According to the report of Kateryna Markevich, a leading expert on economic and social programs, the following threats to the digitalization of SMEs can be identified [7]:

1. Software failure.

Almost every SME now places orders, processes sales and after-sales service, and manufactures products using specialized software. Therefore, a software failure can lead to the impossibility of operating the enterprise.

2. The spread of new methods of mind manipulation.

Due to the easier means of obtaining information, there is too much of it in a person's life. Both positive and negative consequences are observed. Among the negative ones are: giving up one's own opinion, receiving false information, polarization of views.

3. The risk of digital discrimination.

For SMEs, this discrimination may be related to the age characteristics of the entrepreneur. If we look back at the 90s, we will see that computers did not exist in enterprise management; document management was usually carried out on paper and stored in cabinets in the offices of management departments. Computers were introduced to SMEs only in the early-mid 90s, which meant that organizations were able to adapt their function to this technological development. After the introduction of a computer into the department, the Internet suddenly appeared, which, in turn, led to an increase in productivity. But Generation X remained less inclined to use digital innovations than, for example, Generation Z, who do not feel the difference between real

and virtual life at all. The main problem in digitalization is the process of understanding the issues and transforming management from the "old-fashioned method" to the digital one. According to Berghaus S., the initial stage – the "fuzzy interface" – in such a deep innovation process is often perceived as uncertain and chaotic, but it can have a great impact on the outcome. Often, managers find it difficult to initiate this process and determine priorities between different activities. Many studies indicate the importance of a digital transformation strategy, but few researchers study the activities that allow us to understand the possibilities of introducing digitalization into management and the possibilities of implementing this strategy [8].

4. Cyberattacks.

In 2023, SMEs experienced cyberattacks on the Ukrainian telecommunications company Kyivstar and the joint-stock company Commercial Bank Privat Bank. The work of most SMEs was disrupted to varying degrees, which raised the question: can technology be considered "smart" if hackers can easily penetrate the system and disable a state-level company? Thus, the growth of digital security risks, in particular regarding data protection, as well as fears of a breach of personal data confidentiality, contribute to increasing distrust in digital technologies.

5. Social aspect. The introduction of automation and robotics may lead to the replacement of manual labor. Due to digitalization, many current jobs may disappear, forcing people to retrain in order to maintain their employability.

I consider it appropriate to summarize the opportunities that open up for SMEs during digital transformation from the Cabinet of Ministers' Order "On Approval of Strategy for the recovery, sustainable development and digital transformation of small and medium-sized enterprises for the period until 2027 and approval of the operational plan of measures for its implementation in 2024–2027. The strategy outlines the following plan of measures to improve the state of digitalization of SMEs:

1. Countering cybersecurity challenges for businesses by increasing the level of knowledge of small and medium-sized enterprises about protection tools, as well as facilitating the transition of businesses from software of Russian origin to alternative solutions. The SBU, responding to a request from the Union of Ukrainian Programmers (DOU), explained why the use of programs created in Russia is dangerous: "The use by state institutions of software products subject to special economic and other restrictive measures (sanctions) creates a real threat of violating the confidentiality, integrity and availability of data processed in automated systems" [9].

2. Promoting the implementation of electronic invoicing (e-Invoicing), which will help small and medium-sized businesses avoid fines, simplify obtaining tax benefits, and support Ukraine's integration into the EU and increase competitiveness in the European market (a single invoice standard is applied for customers in all EU member states). The Comarch e-Invoicing solution automates invoicing processes related to sales and purchases, ensuring secure data exchange with partners and customers. The automation of this process is not intended to replace employees, but allows accountants to focus on tasks that require human experience and analysis, such as managing exceptional situations or communicating with customers. Accountants who use e-Invoicing automation tools get rid of routine and monotonous tasks. However, in my opinion, such services are most suitable for companies with a large volume of invoices (thousands per month), while small businesses may need them less.

3. Support the introduction of alternative payment methods, including instant payment services, which will help reduce the costs of non-cash transactions and improve the customer experience. According to the NBU, instant payments are payment transactions that are carried out between user accounts in a few seconds using convenient methods of exchanging details and initiating payments [10]. The introduction of instant payments will

contribute to the development of non-cash payments in the country, meet the needs of the market and users, and will also have a positive impact on the level of financial inclusion. In addition, instant payments will become the basis for further modernization of the financial market of Ukraine.

The implementation of instant payments in Ukraine is based on the electronic payments system of the National Bank of Ukraine (SEP), which operates on the basis of the international standard ISO 20022, and using modern European payment schemes Single Euro Payments Area (SEPA). This will simplify future integration into the European Union payment ecosystem and will provide Ukrainians with the opportunity to make not only domestic, but also cross-border instant payments [10].

1. Ensuring the assessment of the level of digital intensity and its increase by collecting, systematizing and publishing key indicators that will characterize digital transformation and integration of digital technologies for small and medium-sized businesses.

How the measurement will be carried out, what indicators will be taken into account, how they are planned to be collected is not currently specified in the strategy document itself. There is also no reference to the methodology for such measurement. The Ministry of Digital Transformation of Ukraine has developed a methodology for measuring the Digital Transformation Index of Ukrainian regions, however, I consider the methodology for measuring the Digital Transformation Index of SMEs to be undisclosed and promising for further research in my scientific works.

2. Implementing data governance policies for SMEs by promoting open data sets and working with technology providers to develop user-friendly data interfaces, analytical tools, and a culture of data (including personal data) and security. These steps will enable SMEs to use open data for market analysis and strategy development.

3. Creating incentives for digital transformation by providing vouchers or grants for investing in digital technologies and

supporting digital skills training. Training vouchers from the State Employment Service will be fully digitalized and available through the Diya portal.

Therefore, when planning the digitalization of a small or medium-sized enterprise, it is necessary to use the strengths of digitalization and analyze how to negate the impact of weaknesses. It is necessary to maximize the emergence of digitalization opportunities using strengths and avoid the emergence of threats (Table 1).

To achieve this goal, it is advisable to use a SWOT analysis as a strategic planning tool that allows for a systematic evaluation of the internal and external factors influencing the digitalization process of the enterprise. Based on the results obtained, key development directions can be identified that leverage the organization's strengths and capitalize on available market opportunities.

Table 1

SWOT analysis of SMP digitalization

1	2	3	4
		Opportunities	**Threats**
	Necessary measures:	1. State support in the development of new digital programs. 2. Support for the implementation of e-Invocing. 3. Support for instant payment service. 4. Development of a methodology for measuring digital transformation. 5. Implementing a data management policy for SMEs.	1. Software failure. 2. The spread of new methods of mind manipulation. 3. Risk of digital discrimination. 4. Cyberattacks. 5. Social risk of replacing certain types of human labor

Table 1 (continued)

1	2	3	4
		6. Providing vouchers for investments in digital technologies. 7. State support for digital skills for SMEs	
Strong	1. The introduction of simplified financial transactions and the growth of the importance of electronic and digital money. 2. Expanding opportunities for remote work. 3. Use of electronic document management. 4. Creating a more transparent and accessible market. 5. Increased production productivity. 6. Reducing the cost of goods and services. 7. Reducing the level of bureaucracy	Simplification of financial transactions already allows instant payments even during bank non-operating hours. Reducing bureaucracy and an open market will allow for more efficient and effective investment in digital technologies	A more open and accessible market for digital services and the possibility of remote work and learning will reduce the risk of digital discrimination of the population
Weak	1. Personal data leak. 2. Computer system failures. 3. Intrusion into private life. 4. Mind manipulation. 5. Increasing digital “inequality” of the population.	The transition from manual data processing to decision support systems, in particular with the use of artificial intelligence technologies (data management), can be complicated by failures	Interference in the privacy of outsiders may pose the risk of new methods of mind manipulation. The risk of substitution of some types

Table 1 (continued)

1	2	3	4
	6. Increasing unemployment	in computer systems and leakage of personal data	of labor may increase the unemployment rate among young people

But first, you need to realize that effective digital transformation is not possible in a team of employees who do not accept innovation. Before integrating digital processes, you need to make sure that the staff is ready to use new technologies and methodologies. To do this, you need to encourage a creative approach to finding solutions that optimize work.

Conclusions. Thus, it can be concluded that considering the issue of digital transformation of SMEs is a very large-scale issue that requires branching into separate segments for research. A fundamentally important point and issue is not only the ways of integrating digital processes, but also understanding the need for use, identifying areas of activity where such integration is possible and promising, preparing SMEs for innovations and ways to overcome "chaos".

References

1. Nechiporenko, K. V., Aleksandrova, M. V. Presentation. Digitization. URL: https://iie.org.ua/wp-content/uploads/2019/02/Prezentatsiya_Margarita-szhatyiy.pdf (date of application: 01.10.2024).

2. Successful implementation. URL: https://unionba.com.ua/solutions

3. Martyniak, I., Bakushevich, I. International experience of business internationalization in the conditions of a knowledge economy. Socio-economic problems and the state. 2021. No. 2(25). P. 564–574. URL: https://doi.org/10.33108/sepd2022.02.564 (access date: 03.10.2024).

4. Khrapkina, V. V. Digital economy and its role in ensuring sustainable economic growth: institutionalization of digital innovations. URL: https://orcid.org/0000-0003-3431-4369 (date of application: 03.10.2024).

5. Oliynyk, I. V. Increasing the sustainability of organizational development of domestic enterprises in the context of digitalization of the economy. Tavria Scientific Bulletin. Series:Economics. 2022. No. 14. P. 37–42. URL: https://doi.org/10.32782/2708-0366/2022.14.5 (date of application: 03.09.2024).

6. Markevich, K. Not only positives. What dangers lie behind digitalization. URL: https://razumkov.org.ua/statti/ne-pozytyvamy-iedynymy-yaki-nebezpeky-kryiutsia-za-tsyfrovizatsiieiu (date of application: 03.10.2024).

7. Order of August 30, 2024 No. 821-rOn approval of the Strategy for Recovery, Sustainable Development and Digital Transformation of Small and Medium-Sized Enterprises for the period until 2027 and approval of the operational plan of measures for its implementation in 2024–2027. URL: https://www.kmu.gov.ua/npas/pro-skhvalennia-stratehii-vidnovlennia-staloho-rozvytku-ta-tsyfrovoi-transformatsii-maloho-i-s821300824 (date of application: 03.10.2024).

8. Berghaus, S., Back, A. Disentangling the fuzzy front end of digital transformation: Activities and approaches. University of St. Gallen; 2017.

9. Sinytska, D. During a full-scale war in Ukraine, accounting programs related to Russia continue to be ordered. URL: https://ti-ukraine.org/blogs/pid-chas-povnomasshtabnoyi-vijny-v-ukrayini-prodovzhuyut-zamovlyaty-buhgalterski-programy-pov-yazani-z-rosiyeyu/ (date of application: 01.10.2024).

10. National Bank of Ukraine. Instant payments. URL: https://bank.gov.ua/ua/payments/ips

11. What are the most common cybersecurity challenges SMEs face today? URL: https://www.helpnetsecurity.com/2021/07/07/smes-cybersecurity-challenges/ (date of application: 01.10.2024).

CHEREP Oleksandr Grigorovich,
Doctor of Economic Sciences, Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0000-0002-3098-0105

MOSTENSKA Tatyana Genadiivna,
Candidate of Economic Sciences, Associate Professor,
National Aviation University, Kyiv, Ukraine
ORCID ID: https://orcid.org/0000-0001-6962-2463

2.4. TRENDS AND PROSPECTS OF DIGITALIZATION IN THE WORLD AND UKRAINE AS A TOOL FOR REBUILDING THE UKRAINIAN ECONOMY IN THE POST-WAR PERIOD

Introduction. During the COVID-19 pandemic and the Russian-Ukrainian war, Ukraine is cooperating with the European Union countries on digital transformation. An example of such digital transformation is the pilot project of a national mobile application based on the "Diya" program to ensure close interconnection with national digital services.

The processes of using digital innovative technologies are also an important tool for increasing accountability and transparency of the reconstruction process and serve as a catalyst for modernization. The goal of Ukraine's digital transformation at the next stage of the state's economic recovery is to increase the share of the IT sector in GDP to 10%. Ukraine's digital transformation is a key driver of economic modernization. Investments in digital innovative technologies will influence the recovery of the economy to increase efficiency, reducing costs in various sectors. The processes of implementing digital innovative technologies in developed countries of the world and in Ukraine cover all sectors of the economy and are reflected in research: Li X Ratti S. [1], Li X Zhang S., Li W. Rickard R., Meng K., Zhang W. [2], Mitchell R. L. [3], Pope D., Sydnor J. [4],

Regeda Y. O., Regeda V. O. [5], Shakir A., Stagemann D., Volk M., Jamus N., Turovsky K. [6], Khaustova V. E., Kryachko E. M., Bondarenko D. V. [7], Yang J. [8], Cherep A. V. [9; 10], Cherep O. G., Gelman V. M., Loseva E. S. [9], Ogrenych Yu. O., Oleinikova L. G., Vasylenko D. O. [10]. Therefore, important are issues that reflect the current state of digitalization in the world and Ukraine.

Presentation of the main research material. The IMD World Digital Competitiveness Ranking (WDCR) 2024, prepared annually by the IMD World Competitiveness Center (WCC), shows how disparities in digital infrastructure development, compounded by the harmful effects of geopolitical tensions, can be compensated by joining the fast-moving flow of new technologies [11].

The GDI (Global Digitalization Index) 2024 tracks the digital development1 of 33 countries and shows a positive correlation between GDI and GDP. The study covers countries that represent a total of 93% of global GDP and 80% of the world's population, which is a good indicator of overall progress in global digital transformation (Table 1).

Table 1

Top 10 countries in the world by GDI in 2024

No.	Country	Index
1	USA	78.8
2	Singapore	76.1
3	Sweden	74.5
4	Finland	73.0
5	Denmark	71.8
6	Switzerland	71.4
7	Netherlands	69.7
8	China	69.2
9	Ireland	68.1
10	Australia	67.6

Source: [11]

As shown in Table 1, the United States topped the ranking among 33 global economies. Singapore came in second and Sweden came in third. Artificial intelligence (AI), blockchain and quantum computing are helping to widen the digital divide, driving innovative change across industries, economies and society as a whole, the ranking report says.

Countries that effectively harness the power of these technologies are likely to increase their digital competitive advantage, leading to sustainable economic growth, improved productivity, and enhanced global influence. Key data sets in the ranking that can be measured include high-tech patents, intellectual property rights, and e-government.

It is the use of high-quality Internet that allows the leading countries of the world to have the highest level of digital transformation (Fig. 1) [12].

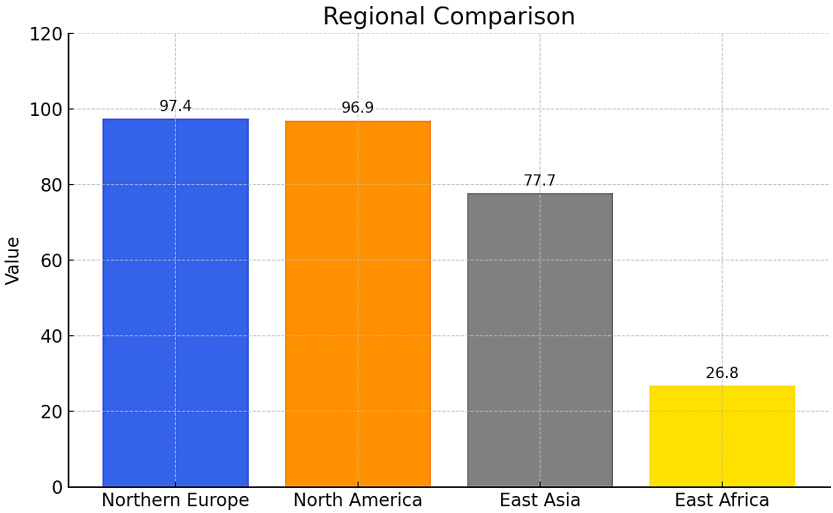

Fig. 1. Internet penetration in the world (%)

Source: [12]

The data in Fig. 1 shows that Northern Europe has the highest Internet usage rates – 97.4%. The lowest Internet usage rates are in East Africa – only 26.8.

Today, Ukraine, despite a number of obstacles (primarily martial law), continues to actively develop the digital sector, introducing the latest technologies. For example, according to research, in 2024, Ukraine's exports of IT services reached 5.31 billion USD, which is 37.7% of total exports of services. Monthly IT exports are 530 million USD. In 2022, this figure was the highest – 600 million USD [13].

In the GDI ranking, Ukraine ranks 60th among 133 economies represented in 2024 [14].

Ukraine also ranks 56th in terms of access to information and communication technologies, but uses them at a lower level (74th place). Online government services are well developed (34th place).

Ukraine ranked fifth in the world in terms of the level of development of digital public services (Table 2).

Table 2

Ranking of countries by level of development of digital public services

Number in the ranking	Country
1	Republic of Korea
2	Denmark
3	Estonia
4	Saudi Arabia
5	Ukraine
6	Singapore
7	Great Britain and Northern Ireland
8	New Zealand
9	Japan
10	Kazakhstan

Source: [15]

Digitalization has already become an integral part of the lives of Ukrainians – the "Diya" application has almost 21 million users, for whom 21 documents and over 30 services are available. Recently, the application became availablemarriage, divorce and name change certificates. On the "Diya" portal, almost 6 million people receive more than 120 services.

At the beginning of 2024, there were 29.64 million Internet users in Ukraine, at which time the penetration rate was 79.2% – the data is based on the assumption of the report's authors that the population of Ukraine at the start of 2024 was 37.4 million people (Fig. 2).

According to the report, from the beginning of 2023 to the beginning of 2024, the population of Ukraine grew by 1.4 million, and the number of Internet users increased by 1 million over the past year. The authors concluded that 7.7 million (or 20%) people in Ukraine do not use the Internet.

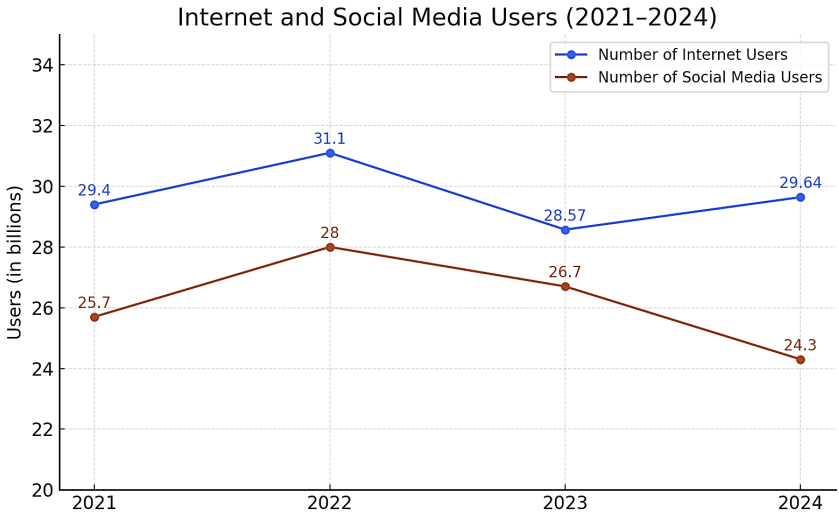

Fig. 2. Number of Internet users in Ukraine

Source: [15]

As shown in Fig. 2, in general, the Internet penetration rate in Ukraine is slightly higher than the global average and is 66%.

In general, digitalization in Ukraine is a rather positive phenomenon for ensuring national security, as the latest technologies help to increase the efficiency of public administration, expand political participation and democratize society. Along with this, such a transformation involves a fundamental change in the forms and mechanisms of functioning of an object or its elements under the influence of internal or external factors.

Mazuruk O. and Poyda S. The main problems of implementing digital initiatives in public administration are considered [17]:

– ensuring digital inclusion: digital transformation must be open to all citizens, especially those with limited access to the Internet or lack the skills to use digital tools, and therefore it is necessary to create conditions for inclusive access to administrative services and digital literacy training;

– transparency: citizens should know exactly how automated digital systems and artificial intelligence work in government institutions, and their use in decision-making processes should comply with approved standards;

– data availability and integration: the ability of government agencies to integrate digital systems, process and exchange data in real time between different departments and institutions requires additional attention and control;

– restoring trust: the potential for manipulation in an unstable digital environment, the likelihood of manipulation in a changing digital space can undermine citizens' trust in public institutions, therefore, authorities must guarantee the responsible use of digital tools and high-quality interaction with citizens.

In confirmation of the fact that strengthening trust should be a priority and one of the most urgent tasks of the country in the near future, there is a study of the study "Assessment of the situation in the country, trust in social institutions,

belief in victory, attitude to elections", which was conducted in March 2024. The results of the trust study show that the state apparatus is often distrusted – namely, distrust is present in 76% of respondents [18].

It is also important to focus on ensuring the reconstruction of Ukraine's economy in the post-war period and increasing the level and development of digital awareness among Ukrainians.

Since the Ministry of Digital Transformation began to actively work on the development of a digital state in 2019, the level of digitalization in the state has increased significantly. Given this, the transformation process has become a priority for the country. The main goal was to implement the "State in a Smartphone" program, which was proposed by Volodymyr Zelensky. The work of the Ministry of Digital Transformation in the public sector has initiated the implementation of many innovations, such as the development of a common IT infrastructure, which is necessary in the process of providing electronic public services. This, in turn, has significantly improved state processes and made them more accessible to society. Therefore, there are a number of advantages in the further process of digitalization of Ukraine.

Accessibility and convenience. Convenience in digital transformation is a fairly broad concept. For some citizens, it is important to have 24-hour access to servers such as Diya and, for example, save time by opening an individual entrepreneur online instead of visiting the ASN. Saving time thanks to online servers has become especially relevant during a full-scale war. This also applies to citizens under temporary occupation or abroad.

Conclusions. Among the ways to overcome the challenges arising in the process of digital transformation of Ukraine, the following technical, socio-cultural and administrative tools are needed [21; 22; 23]:

– training and awareness of employees on digital technologies and cybersecurity. Awareness of the opportunities leads to strategic

planning in implementation, identification of specific steps and responsible persons. This systematic approach ensures efficiency throughout the process. Implementation of information campaigns and development of specialized training programs and courses will help staff adapt to new technologies and processes;

– cost-benefit analysis – the implementation of this phenomenon in all areas should be preceded by a comprehensive analysis of costs and expected benefits throughout the entire life cycle of the asset. This will help to understand the economic feasibility of the project, determine the optimal level of investment and formulate an investment justification;

– phased implementation and management – instead of a large-scale one-time implementation of digital innovations, a phased approach can be considered, using pilot projects to assess effectiveness and address any issues and shortcomings before scaling up, significantly reducing risk;

– data standardization and systems integration: using the best global practices in data processing and integration of various systems, the application of standards will allow standardizing the process of creating digital duplicates, thereby reducing costs and ensuring their continuity and accuracy.

References

1. Li, X Ratti C. Mapping the spatial distribution of shade provision of street trees in Boston using Google Street View panoramas. Urban For Urban Green, 2018, 31: 109–119. URL: https://www.sciencedirect.com/science/article/abs/pii/S1618866717302789

2. Li, X. Zhang C., Li, W. Ricard R., Meng, Q., Zhang, W. Assessing street-level urban greenery using Google Street View and a modified green view index. Urban For Urban Green, 2015, 14: 675–685. URL: https://senseable.mit.edu/treepedia/treepedia_publication.pd

3. Mitchell, R. L. 8 big trends in big data analytics. URL: https://www.computerworld.com/article/2690856/8-big-trends-in-big-data-analytics.html

4. Pope, D., Sydnor, J. Implementing Anti-Discrimination Policies in Statistical Profiling Models. American Economic Journal: Economic Policy. 2011. Vol. 3. P. 206–301. URL: https://pdfs.Semantic

5. Regeda, Yu. O., Regeda, V. O. Key problems of using big data in information systems at the current stage of development. Scientific notes of the V. I. Vernadsky TNU. Series: Technical Sciences. P. 182–187. DOI: https://doi.org/10.32782/2663-5941/2024.4/27. URL: https://www.tech.vernadskyjournals.in.ua/journals/2024/4_2024/29.pdf

6. Towards a concept for building a big data architecture with microservices / Shakir A., Staegemann D., Volk M., Jamous N., Turowski K. Business information systems. 2021. P. 83–94. URL: https://www.researchgate.net/publication/352944091_Towards_a_Concept_for_Building_a_Big_Data_Architecture_with_Microservices

7. Khaustova, V. E., Kryachko, E. M., Bondarenko, D. V. Modeling the impact of digitalization factors on the economic development of countries around the world. Problems of Economy No. 2(60), 2024. Pp. 61–73. URL: https://www.problecon.com/export_pdf/problems-of-economy-2024-2_0-pages-61_73.pdf

8. Yang, J. Big data and the future of urban ecology: From the concept to results. Science China Earth Sciences. 2020. No. 63(10). P. 1443–1456. URL: https://dds.sciengine.com/cfs/files/pdfs/view/1674-7313/6603C72F0F64427 3839EF C754C507C60-mark.pdf

9. Cherep, A. V., Cherep, O. G., Gelman, V. M., Loseva, E. S. European vectors of digitalization of the economy to ensure national security of the state. Publishing house "Young Scientist". No. 11(123) November 2023. URL: https://molodyivchenyi.ua/index.php/journal/article/view/5951

10. Cherep, A. V., Ogrenych, Yu. O., Oleinikova, L. G., Vasylenko, D. O. Financial market of Ukraine in conditions of digitalization of the economy: current state, problems and prospects: collective monograph "Implementation of the European vector of development of the state economy through digitalization" / edited by A. V. Cherep, I. M. Dashko, Yu. O. Ogrenych, O. G. Cherep, V. M. Gelman. Zaporizhzhia: publisher of FOP Mokshanov V. V., 2024. 290 p. P. 252– 263. ISBN 978-617-8064-46-4. DOI: https://doi.org/10.5281/zenodo.14229509

11. World Digital Competitiveness Ranking. URL: https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/

12. 2/3 of the planet's inhabitants are online and the ranking of offline countries – what will we do on the Internet in 2024? URL: https://cases.media/en/article/kozhen-tretii-meshkanec-planeti-onlain-ta-reiting-oflain-krayin-shomi-robimo-v-interneti-u-2024-roci?srsltid=AfmBOorEkwlS69bop9_OuYQ9-gXCEmsn69DkZeqrvwP8IQNR20_2v9NR

13. It is known how much Ukraine earns from exporting IT services – data from Opendatabot. URL: https://vctr.media/ua/vidomo-skilky-zaroblyaye-ukrayina-vid-eksportu-it-poslug-dani-opendatabot-254170/

14. Ukraine ranking in the Global Innovation Index 2024. URL: https://www.wipo.int/gii-ranking/en/ukraine

15. Ukraine topped the world ranking in the use of online government services. URL: https://par.in.ua/information/news/378-ukraina-ocholyla-svitovyi-reitynh-z-vykorystannia-onlain-derzhposluh

16. How a full-scale war affected the number of Internet users in Ukraine. URL: https://www.slovoidilo.ua/2024/04/15/infografika/suspilstvo/yak-povnomasshtabna-vijna-vidobrazylasya-kilkosti-internet-korystuvachiv-ukrayini

17. Mazuruk, O., & Poida, S. (2023). Influence digital tools on changes in modern times public management: mateMNL conference results (15 Dec. 2023, Ivano-Frankivsk), 109–111.

18. Results of the Razumkov Center study "Assessment of the situation in the country, trust in social institutions, belief in victory, attitude to the elections". URL: https://razumkov.org.ua/novyny/otsinka-sytuatsii-v-kraini-dovira-do-sotsialnykh-instytutiv-vira-v-peremogu-stavlennia-do-vyboriv-berezen-2024r

19. Challenges, benefits and prospects of digitalization in Ukraine: Kitsoft CEO for SPEKA. URL: https://kitsoft.ua/ua/news/vikliki-perevagi-i-perspektivi-cifrovizaciyi-v-ukrayini-ceo-kitsoft-dlya-speka

20. Ukraine 2030E – a country with a developed digital economy. URL: https://strategy.uifuture.org/kraina-z-rovizuntoyu-cifrovoyu-ekonomikoyu.ht

21. Akulyushina, M. O. Prospects for the development of the digital economy in Ukraine. Economy and Society. No. 61, 2024. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3724/3646

22. Digital tools for Ukraine's recovery. How to ensure transparent and smart management of reconstruction? URL: https://biz.ligazakon.net/news/218699_v-ukran-rozroblyat-nov-tsifrovnstrumenti-yak-dozvolyatimut-montoriti-construction-process/

23. Yahori, Ya. Ukrainians leave Google to help the Armed Forces of Ukraine. How the military-tech market is growing in Ukraine. URL: https://www.epravda.com.ua/publications/2022/10/26/693086/.26.10.2022

CHEREP Oleksandr Grigorovich,
Doctor of Economic Sciences, Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0000-0002-3098-0105

MOSTENSKA Tatyana Genadiivna,
Candidate of Economic Sciences, Associate Professor,
National Aviation University, Kyiv, Ukraine
ORCID ID: https://orcid.org/0000-0001-6962-2463

2.5. ARTIFICIAL INTELLIGENCE IN THE FIGHT AGAINST PROPAGANDA AND FAKE NEWS. PROSPECTS FOR DEVELOPMENT

Introduction. The article discusses the problem of the spread of fake news and propaganda in the modern digital environment. It analyses the methods and means by which artificial intelligence detects fake texts, images, videos and audio. The principles of algorithm operation are demonstrated: recognition of linguistic structures, analysis of visual inconsistencies, verification of facial expressions and sound signals. The mechanisms of AI operation in popular platforms (Facebook, YouTube) that use neural networks to block fake content are revealed.

Particular attention is paid to the activities of fact-checking platforms such as Logically and The Factual, which combine AI with

expert assessment to verify the accuracy of information. The dynamics of the development of software for detecting fake images are identified, as well as the sources of funding for these technologies: examples of investments by Doppel, Pindrop, Hive AI and state support in the EU, the US and South Korea.

The prospects for the development of artificial intelligence in the context of information security are outlined. The importance of controlling and improving AI algorithms is noted, as well as the likelihood of a transition to quantum computing as the next stage in the fight against information manipulation. A conclusion is made about the effectiveness of AI as a tool for analysing information, which, under proper control, can significantly improve the quality of the information space.

Therefore, the problematic issues of the impact of AI on economic processes were studied by well-known scientists, namely: Borecki J. [1], Dashko I. M. [2; 5; 10], Cherep O. G. [2; 5–10], Kaliuzhna Y. V., Maltiz V. V., Mykhailichenko L. V. [2], Pamment J., Nothhaft H., Fjällhed A. [3], Mlinac N., Akrap G., Lasić-Lazić J. [4], Bekhter L. A. [5; 8; 9], Pidlisnyi R. O. [5], Cherep A., Ogrenych Y., & Kurchenko M. [7], Oleynikova L. G., Veremeenko O. O. [8; 9], Gelman V. M. [9], Vovk M. O. [10]. But the problems associated with the use of artificial intelligence (AI) remain unresolved.

Presentation of the main research material. Today, most people in the world are constantly surrounded by sources of information, each of which in one way or another influences our consciousness, perception of the world and events in it. There are also various ways of presenting information – social networks, news sites, messengers. At the same time, it is important to understand that all information has its own purpose, and this purpose is not always to provide people with truthful information. ‘Whoever owns information owns the world.’ To this statement, it is worth adding a continuation: ‘It doesn’t matter what kind of information it is, as long as people see the truth in it.’ With this approach, most sources of information contain fake news,

and because of the sheer volume of it, people lose their bearings in the information space.

Human efforts alone may not be enough to combat false information – while a person is researching the veracity of information, even more fake news may appear. Because of this, it's impossible to fully control the information space. Instead, we should use modern approaches to fight this problem, like artificial intelligence. Unlike humans, artificial intelligence can process huge amounts of information at once and spot fake news way faster than people can.

To consider the possibilities of artificial intelligence, it is first necessary to examine the types and purposes of fake information. Usually, this is propaganda aimed at manipulating people's perception of political events. This is very relevant now in the context of the war in Ukraine. The main goal of such manipulation is to cause panic in Ukraine and spread it further. Another goal is to shape false public opinion in order to intensify aggression between one nation and another.

In this example, the capabilities of artificial intelligence begin to manifest themselves in the analysis of textual information. There are verified sources of information that have existed for years. The information from them is considered the basis against which new information is compared. When analysing data, artificial intelligence detects signs of fabricated information and flags them as potentially fabricated. A team of experts then works with the flagged data to make a final conclusion about the veracity or fictitiousness of the information.

Fake images and videos are also common on the internet. Artificial intelligence also has its own tools for such purposes. It analyses photos and videos, taking into account lighting, gestures and facial expressions. Since these factors are interrelated, they can affect the image or voice, and artificial intelligence takes all contradictions into account. An example would be images in which the lighting is unevenly distributed relative to the light source, indicating that

a certain element has been added to the image by another person or software [11].

Videos can also be created by humans or even artificial intelligence (a video superimposed on another image, with added elements, or a completely edited video). Here, too, inconsistencies are recorded, and the video is marked as potentially fake.

The detection procedure is similar for voice. When certain sounds are pronounced, the face also moves. The voice and facial expression recognition programme detects when these factors do not match and flags the audio file as potentially fake [12].

But that's not all artificial intelligence can do. There is also a need to check text documents. Text styles and speech styles are used to recognise propaganda. Each style has its own writing and structural characteristics. Artificial intelligence recognises key phrases and words that indicate a particular style. When words that are potentially unacceptable, violent or propagandistic are detected, artificial intelligence flags them [13].

One of the most popular sources of information today is social media, where the spread of fake news is particularly effective for a wide range of users. At the same time, the introduction of artificial intelligence accelerates and automates the process of identifying posts with potentially unacceptable content or posts inciting hatred.

Facebook is a good example. Neural networks recognise the data in posts and automatically block them. Facebook's neural network filtering works in over 50 languages, scaling the effectiveness of filtering fake posts to the entire target audience.

YouTube is another good example. Neural networks automatically block information that contains personal propaganda or the promotion of certain products. It is worth noting that this network actively supports the implementation of artificial intelligence in video content. This is evidenced by the fact that videos generated or voiced by artificial intelligence are becoming more and more common. These videos have a similar structure and are easier for viewers

to understand. But often, one video can have different voiceovers with completely different meanings. So, someone's post can fall victim to artificial intelligence, which makes it even harder for viewers to understand the info and figure out what's true.

Therefore, it is quite important to have a publication admission policy that creates or limits the possibilities for creating and publishing photos, videos or text materials. When supporting content created by artificial intelligence and humans, it is worth developing a filter for content that is potentially desirable to the viewer so that it is not difficult to perceive. In this case, it will be easier for consumers to distinguish between factual and generated information. Thus, social networks will become an informational and entertainment space where each viewer can find content for their own specific purposes.

To verify the accuracy of information, there are fact-checking platforms, such as Logically, a platform based in the UK. It works in two stages: the platform's artificial intelligence simultaneously checks large volumes of publications and compares them with news, forums and social networks. After analysing the data, the artificial intelligence sends the results of the verification to a team of experts, who make the final conclusion about the accuracy of the information.

This is one of the methods of combating fake news, which consists of verifying news by comparing it with official sources of information. However, this platform verifies news that has already been published, but does not minimise its dissemination among viewers in the event of invalid information being detected.

Another example with more features is The Factual. It evaluates publications based on several criteria: the authority of the source, the validity of the material, and the style of presentation. Based on these criteria, the news item receives a score from 0 to 100 points, which serves as a rating for the viewer. This platform checks over 10,000 news items around the clock. In fact, it is a filter for potentially desirable content for the consumer.

This service can also be used by the viewer themselves. Thanks to The Factual, they can independently check the news that interests them. This is the most effective method of combating fakes and propaganda, as it is aimed directly at the target audience and the product they use.

It is also worth noting the importance of funding such projects. Projects aimed at creating systems for detecting fake information require significant and stable investments. This is due to the complexity of the tasks that such development sets for itself: it covers not only programming, but also in-depth interdisciplinary research in the fields of artificial intelligence, machine learning, linguistics, and the psychology of information perception. One of the main stages is training algorithms on large amounts of high-quality data, which requires the creation, verification, and constant updating of databases of reliable information. In addition, it is important to ensure the integration of such solutions with existing news platforms, social networks, and services for effective and rapid filtering of harmful content.

Financial support from governments, international institutions, and technology businesses allows not only to maintain the functioning of existing systems, but also to expand their capabilities. This includes scaling infrastructure, improving detection accuracy, adapting to different languages and cultures, and developing new tools.

Software products for detecting fake images are also gaining momentum. As of now, funding for fake image detection software in 2024 amounted to $0.6 billion. By 2029, this amount is projected to grow to $3.9 billion. The leaders in fake image detection are the following corporations [14]:

– Microsoft Corporation (United States);
– Gradiant (Spain);
– Facia (United Kingdom);
– Image Forgery Detector (Belgium);
– Q-integrity (Switzerland);

– iDenfy (Lithuania);
– DuckDuckGoose AI (Netherlands);
– Primeau Forensics, Sentinel AI (Estonia).

With regard to the detection of video and audio fakes, it is worth noting the regular involvement of funds. In 2024, Doppel received $35 million in funding, and Pindrop received $100 million in debt financing from Hercules Capital to develop the detection of fake voices [15].

Friedrich-Alexander University in Erlangen-Nuremberg received preliminary funding of €350,000 to develop a project for detecting images generated by artificial intelligence. In the same field, Hive AI received $2.4 million in funding from the US Department of Defence [16].

Many organisations receive funding from governments and other organisations to detect fake images, videos and audio. This shows the relevance of this topic and the growing rate of fake content creation in the world.

Artificial intelligence acts as a filter in detecting fake news, articles, photos, videos and audio materials. It is impossible for a human to process that amount of information at the same speed. In addition, there is the problem of creating fake content with artificial intelligence. It itself operates according to certain algorithms, and it will also be quicker to detect the program code that caused the false information to appear, because a human only sees the result (photo, video or text), not the program code itself.

For further development, it is worth considering the theory of creating a quantum computer. For a clearer understanding, imagine a maze with many branches. A conventional computer or human must check different paths one by one to find the exit. But a quantum computer can do this much faster.

Quantum bits can exist simultaneously in several states specified by the algorithm. Thanks to this, a quantum computer can explore all paths at once, rather than sequentially, like a conventional computer.

Using a quantum algorithm, the system quickly finds the way to the exit, cutting off unsuccessful routes without having to return to another path. In other words, a quantum computer goes in all available directions to try to find the exit simultaneously, without stopping when it hits a wall.

Thus, the quantum approach is a modern, improved form of the heuristic trial and error method, but in our case, it is the detection of fake and true information.

Given that this technology is not currently available, it is worth improving artificial intelligence algorithms to speed up the detection of deviations and increase the number of publications for simultaneous analysis. In this case, a database of potentially suspicious publications will be created. Considering that artificial intelligence can also make mistakes, potential fakes should be checked again using the same principle. This can reduce the amount of work for people who carry out control.

Conclusions. Thus, artificial intelligence is an effective tool for combating fakes, significantly speeding up the process of detecting them. Its effectiveness is evident in the analysis of images, videos and text documents. However, the use of artificial intelligence must be accompanied by human control, as artificial intelligence is also prone to errors.

Every year, the problem of detecting fake content becomes more acute due to the emergence of new means of creating it. Because of this, governments of various countries are funding projects and start-ups to detect false or fabricated information, videos and photos. The leaders in detecting fake publications are the United States, Great Britain, Spain, Belgium, Switzerland, Lithuania, the Netherlands and Estonia.

In the longer term, in the context of the development of the topic under study, quantum technologies based on advanced algorithms were considered, which would cover a larger volume of data verification and significantly speed up the detection of fake publications, minimising the need for human control.

References

1. Borecki, J. (2024). Disinformation as a threat to private and public enterprises, URL: https://surl.li/ckvnie

2. Dashko, I. M., Cherep, O. G., Kaliuzhna, Y. V., Maltiz, V. V., Mykhailichenko, L. V. Artificial Intelligence as a Tool for Countering Disinformation in Wartime: Experience and Prospects of Application in Ukraine. Topical issues of economic sciences, 2025. (7). DOI: https://doi.org/10.5281/zenodo.14760314. URL: https://a-economics.com.ua/index.php/home/article/view/185

3. Pamment, J., Nothhaft, H., and Fjällhed, A. (2024). Countering informationinfluence activities: the state of the art. URL: https://surl.li/bdeebp

4. Mlinac, N., Akrap, G., Lasić-Lazić, J. (2021). Novi oblici manipuliranja udigitaliziranom prostoru javnog znanja i potreba za uspostavom digitalnog ipodatkovnog suvereniteta. National Security and the Future, Vol. 21. No. 3, 2021. P. 27–63 DOI: 10.37458/nstf.21.3.1. URL: https://www.researchgate.net/publication/349934213_Novi_oblici_manipuliranja_u_digitaliziranom_prostoru_javnog_znanja_i_potreba_za_uspostavom_digitalnog_i_podatkovnog_suvereniteta

5. Cherep, O. G., Dashko, I. M., Bekhter, L. A., Pidlisnyi, R. O. Advantages and Challenges of Digitalization of the Economy of Ukraine. Technology. 2024. No. 1(9). P. 131–135. URL: http://ujae.org.ua/wp-content/uploads/2024/02/ujae_2024_ r01_a21.pdf

6. Cherep, O. G. Accelerating Digitalization and COVID-19: A Retrospective Review and Impact on New Job Creation. International scientific journal "Internauka". Series: "Economic Sciences". 2023. № 4. DOI: https://doi.org/10.25313/2520-2294-2023-4-8825. URL: https://www.inter-nauka.com/issues/economic2023/4/8825

7. Cherep, A., Cherep, O., Ogrenych, Y., & Kurchenko, M. Denmark's Experience in Digitalization of Business Processes as an Example for Ukraine. Herald of Khmelnytskyi National University. Economic Sciences, 2024, 324(6). P. 164–168. DOI: https://doi.org/10.31891/2307-5740-2023-324-6-26. URL: https://heraldes.khmnu.edu.ua/index.php/heraldes/article/view/294/302

8. Cherep, O. G., Oleynikova, L. G., Bekhter, L. A., Veremeenko, O. O. Digitalization of the economy in Ukraine and Europe: current state,

problems and limitations, collective monograph "Digitalization as a tool for ensuring the quality of educational services taking into account the European experience" / ed. A. V. Cherep, I. M. Dashko, Y. O. Ogrenich, O. G. Cherep. Zaporizhzhia: publisher FOP Mokshanov V. V., 2024. 300 p. P. 86–97. ISBN 978-617-8064-50-1. DOI: https://doi.org/10.5281/zenodo.14258696

9. Gelman, V. M., Cherep, O. G., Bekhter, L. A., Veremeenko, O. O. Innovations in the field of digitalization as a driving force of socio-economic changes in the EU countries. Collective monograph "Implementation of the European vector of development of the state's economy through digitalization" / A. V. Cherep, I. M. Dashko, Y. O. Ogrenych, O. G. Cherep, V. M. Gelman. Zaporizhzhia: publisher FOP Mokshanov V. V., 2024. 290 p. P. 116–123. ISBN 978-617-8064-46-4. DOI: https://doi.org/10.5281/zenodo.14229509

10. Cherep, O. G., Dashko, I. M., Vovk, M. O. Digitalization Tools in Financial Resources Management. Artificial Intelligence and Digital Technologies in the Transformation of the Economy of Ukraine in the Period of War and Post-War Recovery: Collective Monograph / ed. O. G. Cherep. Zaporizhzhia: Publisher FOP Mokshanov V. V., 2025. 238 p. P. 107–117.

11. How to detect Fake News with AI | Founderz. Founderz. URL: https://founderz.com/blog/detecting-fake-news-with-ai/ (date of access: 16.06.2025).

12. Turner, M. How clever app can spot deepfake videos in latest battle against AI clones. The Sun. URL: https://www.thesun.co.uk/tech/30562824/deepfake-detector-app-mcafee-ai-videos/ (date of access: 16.06.2025).

13. Rogers, R. Real-Time Video Deepfake Scams Are Here. This Tool Attempts to Zap Them. WIRED. URL: https://www.wired.com/story/real-time-video-deepfake-scams-reality-defender/ (date of access: 16.06.2025).

14. Ltd M. R. P. Fake Image Detection Market worth $3.9 billion by 2029, growing at a CAGR of 41.6%: Report by MarketsandMarkets™. GlobeNewswire News Room. URL: https://www.globenewswire.com/news-release/2024/04/11/2861611/0/en/Fake-Image-Detection-Market-worth-3-9-billion-by-2029-growing-at-a-CAGR-of-41-6-Report-by-MarketsandMarkets.html (date of access: 16.06.2025).

15. New Funding Rounds in Deepfakes | VentureRadar. VentureRadar. URL: https://www.ventureradar.com/funding/Deepfakes (date of access: 16.06.2025).

16. Borak, M. DoD awards contract for deepfake detection to Hive | Biometric Update. Biometric Update | Biometrics News, Companies and Explainers. URL: https://www.biometricupdate.com/202412/dod-awards-contract-for-deepfake-detection-to-hive (date of access: 16.06.2025).

CHEREP Oleksandr Grigorovich,
Doctor of Economics, Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0000-0002-3098-0105

KALIUZHNA Yuliia Viktorivna,
Candidate of Economic Sciences, Associate Professor,
Zaporizhzhia National University, Zaporizhzhia, Ukraine
ORCID: https://orcid.org/0000-0002-3335-6551

2.6. MECHANISMS OF ARTIFICIAL INTELLIGENCE FOR DETECTING COORDINATED INFORMATION ATTACKS

Introduction. In the modern digital age, the proliferation of information technologies has significantly transformed communication, enabling rapid dissemination of data across the globe. While this transformation has brought numerous benefits, it has also facilitated the emergence of new threats, including coordinated information attacks (CIAs). These attacks are deliberate efforts by malicious actors to manipulate public opinion, destabilize social or political systems, or discredit individuals and organizations. The complexity and scale of these attacks have made traditional detection methods insufficient. Consequently, the development of advanced artificial intelligence (AI) mechanisms for identifying and mitigating such threats has become a priority in cybersecurity and information security domains.

This paper explores the role of AI in detecting CIAs. It examines various machine learning (ML), deep learning (DL), and natural

language processing (NLP) techniques that can be employed to uncover patterns, anomalies, and coordinated behaviors indicative of an information attack. Through a comprehensive review of existing literature, the article highlights the strengths and limitations of current approaches and proposes potential avenues for future research and improvement.

Presentation of the Main Research Material.

1. Understanding Coordinated Information Attacks.

Coordinated information attacks involve the orchestration of multiple accounts, often automated or semi-automated, to spread misleading or harmful information. These attacks can target political events, elections, public health, or corporate reputations. Tactics include the use of fake news, deepfakes, botnets, and troll farms.

CIAs are typically characterized by:

– Synchronization: Simultaneous posting or sharing of similar content.
– Amplification: Boosting the visibility of specific narratives.
– Inauthentic behavior: Use of bots or fake profiles.
– Obfuscation: Efforts to conceal coordination.

Coordinated Information Attacks (CIAs) represent a strategic and often covert manipulation of the digital information environment with the goal of influencing public perception, disrupting social consensus, or undermining institutions. Unlike isolated instances of misinformation or random online discourse, CIAs are systematic, well-orchestrated campaigns that deploy multiple vectors-such as automated agents (bots), compromised human accounts, and coordinated messaging-to amplify specific narratives or disrupt the spread of accurate information.

A fundamental characteristic of CIAs is the deliberate and synchronized effort among various actors, frequently involving both automated and human participants. These campaigns are typically executed across multiple platforms, taking advantage of the interconnectivity of modern digital ecosystems to maximize

reach and impact. Targets of such attacks range from political processes, such as elections and referenda, to public health initiatives, corporate reputations, and social movements. The intent behind CIAs can be multifaceted-political influence, financial gain, ideological warfare, or reputational sabotage.

Operationally, CIAs exhibit several identifiable traits. Synchronization refers to the tight timing coordination among participating accounts, which may include posting identical or thematically similar messages within seconds or minutes of each other. Amplification occurs when large numbers of accounts engage with specific content through likes, shares, retweets, or comments to artificially inflate its visibility. Inauthentic behavior is another hallmark, often involving fake profiles, sockpuppet accounts, or botnets that operate in a coordinated manner to mimic organic activity. Obfuscation strategies are also frequently employed to conceal the true origins of the campaign, including the use of VPNs, disposable accounts, linguistic camouflage, and overlapping digital fingerprints.

CIAs can be classified into several categories based on their objectives and techniques. Disinformation campaigns aim to disseminate false or misleading content with the intent to deceive, often blending factual information with lies to increase credibility. Influence operations seek to shape public attitudes or decisions through psychological manipulation and narrative framing. Astroturfing creates the illusion of grassroots support or opposition by orchestrating mass messaging from fake personas. Meanwhile, narrative laundering involves the repetition and gradual normalization of fringe or harmful ideas by injecting them into mainstream discourse via coordinated amplification.

The scale and sophistication of CIAs have grown substantially with the advent of advanced technologies. Artificial intelligence itself is now being weaponized by malicious actors to generate realistic content (such as deepfakes), optimize posting schedules, and evade detection mechanisms. Moreover, the rise of decentralized and

encrypted platforms complicates monitoring efforts, allowing threat actors to coordinate in private channels before disseminating content publicly. The internationalization of these operations also poses challenges, as campaigns may originate in one jurisdiction and target audiences in another, often exploiting regulatory and linguistic gaps.

Understanding the anatomy and behavior of CIAs is crucial for developing robust defense mechanisms. It requires a multidisciplinary approach that combines insights from cybersecurity, data science, linguistics, sociology, and political science. Only by accurately modeling how coordinated attacks unfold, what signals they emit, and how they adapt under pressure, can AI-driven detection systems be effectively designed to counter them.

In sum, coordinated information attacks are a growing threat to the integrity of public discourse and democratic processes. Their detection and mitigation demand sophisticated analytical tools capable of parsing complex patterns, high-volume data, and subtle indicators of inauthentic behavior. The sections that follow delve into how artificial intelligence can fulfill this role, offering scalable and adaptive solutions to safeguard the digital information environment.

2. Role of AI in Detecting CIAs.

Artificial Intelligence (AI) plays a transformative role in the detection of Coordinated Information Attacks (CIAs), offering capabilities that far exceed traditional analytical tools in scale, speed, and adaptability. In contrast to manual monitoring or rule-based detection systems, AI models can autonomously analyze massive volumes of data from diverse platforms in real-time, recognize evolving threat patterns, and continuously adapt to new tactics used by malicious actors.

AI's effectiveness stems from its ability to integrate multiple subfields of computational intelligence-machine learning (ML), deep learning (DL), and natural language processing (NLP)-into cohesive systems that work synergistically. Each component offers distinct analytical strengths that, when combined, enable a comprehensive

understanding of both surface-level indicators and deep structural patterns associated with CIAs.

A. Machine Learning (ML).

Machine learning is fundamental in classifying content and behaviors based on historical data. Supervised learning algorithms, such as logistic regression, support vector machines (SVM), and random forests, are often trained on labeled datasets of known malicious and benign activities. These models are effective at detecting recurring indicators, such as coordinated hashtag usage or repetitive phrasing, that suggest manipulation.

In contrast, unsupervised learning models-such as k-means clustering, DBSCAN, and autoencoders-allow the discovery of hidden groupings or anomalies without pre-existing labels. These methods are particularly valuable in detecting novel or previously unknown forms of coordination, as they can identify subtle relationships between accounts or content that would otherwise go unnoticed.

Semi-supervised and self-supervised learning approaches are also gaining traction, as they can leverage large quantities of unlabeled data while requiring minimal manual annotation. This is crucial in contexts where obtaining labeled datasets is difficult due to privacy concerns or the constantly evolving nature of disinformation.

B. Deep Learning (DL).

Deep learning models, especially neural networks, offer powerful tools for capturing complex, non-linear relationships within unstructured data such as text, images, and user behavior logs. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are effective for modeling temporal sequences, enabling the detection of coordination patterns that unfold over time. For example, these models can identify repeated message propagation sequences or unnatural synchronization across accounts.

Convolutional Neural Networks (CNNs), though traditionally used for image analysis, can also be adapted to detect spatial patterns in activity graphs or content similarity matrices. More recently,

transformer architectures-such as BERT, RoBERTa, and GPT-have revolutionized text understanding by enabling context-aware semantic analysis. These models can parse not only what is being said, but how and why it is being communicated, which is critical in identifying covert agendas or emotional manipulation strategies.

Moreover, deep learning facilitates the generation of embeddings-dense vector representations of content or user behavior-that can be clustered, compared, or used as features in higher-level classification tasks. These embeddings help identify semantically similar messages, even when surface-level wording differs, revealing disguised coordination.

C. Natural Language Processing (NLP).

NLP enables AI systems to interpret, analyze, and contextualize textual data at scale. Techniques such as sentiment analysis can identify the emotional tone of messages, which is often manipulated in CIAs to incite outrage, fear, or distrust. Named Entity Recognition (NER) helps track how specific individuals, organizations, or events are being portrayed, while topic modeling and semantic clustering reveal dominant narratives being pushed by potentially coordinated accounts.

Importantly, NLP tools can also be used to detect stylometric patterns-distinctive linguistic styles or syntactic structures that suggest common authorship or script-based message generation. By analyzing lexical richness, grammatical construction, and phrase reuse, AI can infer whether multiple accounts are disseminating content generated from the same template or script.

Multilingual NLP models further enhance detection capabilities across different linguistic and cultural contexts, allowing AI systems to track disinformation in global campaigns that operate in multiple languages simultaneously.

3. Visual Model of the AI Detection Mechanism.

In order to better illustrate the operational logic behind artificial intelligence systems used for the detection of coordinated information attacks (CIAs), a conceptual diagram has been developed (Fig. 1).

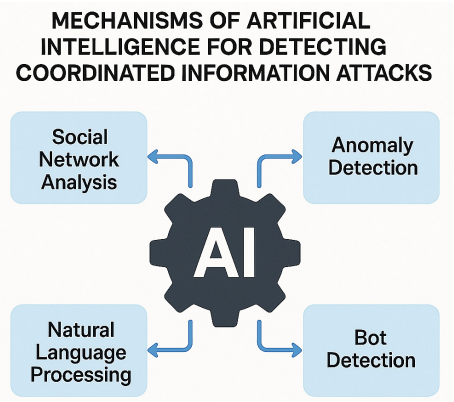

Fig. 1. Mechanisms of Artificial Intelligence
for Detecting Coordinated Information Attacks

This schematic representation places the AI engine at the core of the detection mechanism, underscoring its role as the central analytical entity that orchestrates the interaction among multiple analytical subsystems. Four principal components-Social Network Analysis, Anomaly Detection, Natural Language Processing, and Bot Detection-are positioned around the central AI unit, each representing a specific operational function critical to identifying malicious coordination.

The central AI hub, depicted as a mechanical gear, symbolizes the autonomous and adaptive nature of artificial intelligence in continuously learning from data and updating its detection models. This AI core receives input from vast streams of digital content and user interaction metadata, which it then processes using advanced machine learning and deep learning techniques. These techniques include supervised classification, clustering, neural embeddings, and sequential modeling, enabling the AI to discern both known patterns of coordinated behavior and emergent, previously unseen tactics.

Surrounding the core AI unit are the four specialized functional modules. The first of these, Social Network Analysis, emphasizes

the structural dimension of CIAs. This component applies graph theory and network analysis to identify clusters of accounts exhibiting high connectivity, synchronized messaging, or mutual amplification behavior. Such structural similarities are often indicative of orchestrated campaigns designed to manipulate information ecosystems. AI enhances this analysis by automatically detecting communities, evaluating network centrality, and assessing information diffusion paths.

The second module, Anomaly Detection, plays a crucial role in identifying statistical outliers and behavioral inconsistencies across user or group activity. AI systems compare observed activity patterns against historical baselines or against the broader behavioral norms of platform users. Sudden bursts in posting frequency, the rapid appearance of identical messages across multiple accounts, or atypical interaction sequences may all serve as indicators of coordinated operations. This module often employs probabilistic models, density estimation techniques, and unsupervised learning algorithms to ensure robustness against evasion techniques.

Natural Language Processing (NLP), another key component, allows the AI system to interpret and analyze textual data at scale. This includes identifying semantic patterns, sentiment polarities, rhetorical structures, and recurring narratives. NLP capabilities are essential for distinguishing between organic discourse and artificial messaging campaigns. For example, coordinated actors frequently reuse linguistic templates or promote identical narratives with slight lexical variation. Transformer-based models such as BERT and GPT play a pivotal role in this module, providing the AI system with contextual understanding of language, enabling accurate content classification, entity tracking, and thematic clustering.

The final component depicted is Bot Detection, which targets the identification of automated and semi-automated agents. Bots play a central role in scaling disinformation operations, often operating in swarms to amplify messages, distort engagement metrics, and

create the illusion of consensus. AI models used in this context analyze posting behavior, account metadata, linguistic uniformity, and timing regularities. By combining these indicators, the system can flag inauthentic activity with high precision, thereby reducing the surface area for successful manipulation.

Together, these four components represent a cohesive and interdependent set of capabilities. The diagram conveys that while each analytical module operates with its own methodological tools, they all feed into and are governed by the central AI unit. This architectural design ensures that the detection system remains holistic, scalable, and capable of rapid adaptation in response to evolving adversarial strategies. The visual model thus supports and clarifies the conceptual framework discussed in the article, reinforcing the argument that only integrated, AI-driven systems are capable of effectively addressing the scale and complexity of modern coordinated information threats.

4. Detection Techniques and Methodologies.

A. Network Analysis.

Social network analysis identifies clusters of accounts exhibiting similar behavior. Techniques like community detection and graph-based anomaly detection are instrumental in revealing coordinated groups.

B. Temporal Pattern Recognition.

Coordinated attacks often follow specific temporal patterns. AI can detect bursts of activity, repetition of content, and time-based correlations between user actions.

C. Content Similarity Analysis.

Using NLP and DL, systems can compare textual and multimedia content to identify duplicated or near-duplicated messages, signaling coordination.

D. Behavioral Modeling.

AI models can learn typical behavior patterns for users or groups. Deviations from the norm may indicate malicious coordination.

5. Case Studies.

Case Study 1: Election Interference

The practical application of artificial intelligence in identifying and mitigating coordinated information attacks can be best understood through real-world case studies. These examples demonstrate how AI-driven methods have been deployed across different domains, highlighting both the capabilities and challenges associated with their implementation.

Case Study 1: Election Interference

One of the most prominent examples of coordinated information attacks occurred during the 2016 United States Presidential Election. Researchers and intelligence agencies revealed a complex web of bots, trolls, and fake accounts used to amplify divisive content, spread misinformation, and influence voter behavior. AI technologies played a vital role in uncovering these activities. Specifically, machine learning models were used to analyze social graph data, revealing clusters of accounts that exhibited synchronized behavior such as retweeting the same content at the same time or using identical hashtags. Natural language processing helped identify the narratives being pushed, and bot detection algorithms flagged accounts with highly regular posting patterns and minimal engagement with authentic users. These insights were crucial in attributing the operation to foreign influence campaigns and in strengthening platform policies around political advertising and misinformation.

Case Study 2: COVID-19 Misinformation Campaigns

The global pandemic brought a surge in health-related misinformation, much of which was coordinated and intended to undermine public trust in health authorities and vaccination efforts. AI systems were deployed by social media platforms and health organizations to counteract these threats. Natural language processing models were instrumental in identifying anti-vaccine rhetoric, false cures, and conspiracy theories. At the same time, anomaly detection algorithms spotted unusual spikes in the sharing of specific misleading posts, often originating from bot-like accounts or networks

of coordinated users. Through a combination of content analysis and behavioral tracking, AI helped platforms down-rank or remove harmful misinformation while also enabling public health bodies to respond with accurate counter-messaging.

Case Study 3: Corporate Disinformation Campaigns

Another application of AI in detecting coordinated attacks involves corporate disinformation, where rival companies or third-party actors attempt to damage a company's reputation through coordinated negative reviews, fabricated news stories, or mass social media campaigns. In one well-documented case, a large electronics firm was targeted by thousands of suspicious social media posts alleging product defects. Using AI-based sentiment analysis and behavioral modeling, the company's cybersecurity team identified that many of the accounts had been recently created, followed similar posting schedules, and recycled language templates. Social network analysis further revealed interconnections between these accounts that suggested a single entity was orchestrating the attack. By presenting this evidence to the platform and the public, the company was able to mitigate reputational damage and initiate legal proceedings.

Case Study 4: Geopolitical Propaganda Operations

State-sponsored disinformation campaigns have become increasingly common in the context of international conflicts and political unrest. AI systems have been used to detect efforts by foreign actors to spread propaganda through coordinated campaigns on platforms such as Facebook, Twitter, and YouTube. One example includes a state-backed network that used a combination of authentic-looking accounts and automated bots to promote a specific political agenda during protests in a neighboring country. AI mechanisms identified the coordination through behavioral signals such as identical posting times, shared URLs, and echo-chamber amplification. Language models were used to trace message similarity, while graph analysis revealed high-density interconnections that far exceeded organic user interaction levels. These findings supported

the suspension of thousands of accounts and a broader understanding of hybrid warfare strategies that combine digital propaganda with traditional geopolitical tactics.

These case studies highlight the multifaceted application of AI in real-world scenarios and demonstrate how various detection mechanisms-ranging from NLP to anomaly detection and social graph analysis-work in tandem to identify coordinated activities. They also emphasize the importance of continuous model adaptation, ethical oversight, and collaboration between AI researchers, platform providers, and policy makers.

6. Challenges and Limitations.

While the deployment of artificial intelligence in detecting coordinated information attacks has shown promising results, several challenges and limitations continue to impede its full potential. These obstacles span technical, ethical, and operational dimensions, and understanding them is crucial to advancing the reliability and accountability of AI-driven detection mechanisms.

A. Data Availability and Quality.

A core challenge in training and validating AI models for disinformation detection lies in the scarcity of high-quality, labeled datasets. Platforms are often reluctant or legally restricted from sharing detailed user data due to privacy concerns and proprietary policies. Moreover, the datasets that are publicly available tend to be limited in scope or biased toward particular languages, regions, or types of attacks. Without representative and diverse datasets, AI models risk underperforming in real-world scenarios or reinforcing systemic biases.

B. Evolving Tactics of Malicious Actors.

Coordinated information attacks are dynamic and adaptive. As detection methods become more advanced, attackers develop new evasion techniques such as using obfuscated language, rotating account usage, or leveraging human-operated accounts to mimic authentic behavior. This constant arms race between detection and

deception necessitates continuous model updates and retraining. Static or outdated models quickly become ineffective, highlighting the need for AI systems that can learn incrementally and adapt to new threats in near-real-time.

C. High False Positive Rates.

Another major limitation of current AI approaches is the potential for false positives-cases where legitimate, grassroots campaigns or coordinated activism are misclassified as malicious operations. This is especially problematic in politically sensitive contexts, where the distinction between organic mobilization and coordinated manipulation can be subtle. Overzealous detection mechanisms risk infringing on freedom of speech and suppressing civic engagement. Striking the right balance between vigilance and overreach is an ongoing challenge for developers and policy-makers alike.

D. Interpretability and Explainability.

Many state-of-the-art AI models, particularly deep learning architectures, are inherently opaque and difficult to interpret. This lack of transparency can hinder trust in AI-generated outputs, especially in high-stakes environments such as national security or journalism. If an AI system flags a network of users as malicious, it must be able to explain why. Research in Explainable AI (XAI) is addressing this gap by developing tools that provide human-understandable reasoning behind decisions, but these methods are still in their infancy.

E. Platform Variability and Integration Complexity.

Social media platforms differ significantly in architecture, data accessibility, user behavior, and content moderation policies. An AI model developed for Twitter may not translate effectively to platforms like TikTok or Telegram. Furthermore, coordinated attacks often span multiple platforms, making cross-platform analysis both technically and logistically challenging. Integrating AI detection mechanisms across varied ecosystems requires standardized protocols, interoperability frameworks, and inter-organizational cooperation.

F. Ethical and Privacy Concerns.

Automated surveillance and behavioral analysis raise important ethical questions, particularly regarding user privacy and consent. Collecting and analyzing large-scale social media data may inadvertently expose personal information or disproportionately target marginalized groups. Developers must navigate regulatory landscapes such as the General Data Protection Regulation (GDPR) and ensure that their models operate within the bounds of ethical data use. Moreover, transparency in how data is collected, stored, and utilized is essential for maintaining public trust.

G. Resource and Expertise Constraints.

Developing robust AI systems for CIA detection requires significant computational resources, skilled personnel, and sustained funding. Smaller organizations, non-profits, or governments in low-resource settings may struggle to deploy or maintain such systems. This creates an uneven playing field in the fight against disinformation, where only well-funded entities can afford to protect themselves against sophisticated attacks.

While artificial intelligence offers powerful tools for detecting coordinated information threats, its limitations must be critically addressed. Future efforts should focus not only on technical advancements but also on fostering ethical standards, enhancing data access and diversity, and ensuring that AI applications are inclusive, transparent, and resilient to adversarial manipulation.

7. Future Directions.

As the landscape of information warfare continues to evolve, the future development of AI mechanisms for detecting coordinated information attacks (CIAs) must address current limitations while anticipating emerging challenges. Several promising research directions and technological innovations can help improve the effectiveness, adaptability, and ethical grounding of AI-based detection systems.

One of the most critical areas for advancement is the integration of real-time detection capabilities. Current systems often operate

with a delay, analyzing patterns after significant damage has already occurred. Future AI architectures should incorporate streaming data analytics and incremental learning models capable of identifying suspicious coordination as it unfolds. This requires not only technical optimization but also collaboration with platform providers to ensure timely access to relevant data.

Another important development lies in the creation of more sophisticated multimodal AI systems. Coordinated disinformation campaigns increasingly combine text, images, videos, memes, and even deepfakes. Detecting such threats will necessitate AI models that can fuse signals across multiple content types and contextual layers. Progress in computer vision, audio analysis, and multimodal fusion techniques will be essential in this regard.

The expansion of multilingual and cross-cultural AI capabilities is also essential. Most current models are trained on English-language datasets, limiting their efficacy in detecting CIAs targeting non-English-speaking populations. Future research must prioritize inclusive language coverage and cultural nuance, leveraging advances in multilingual large language models and cross-lingual transfer learning.

Furthermore, explainability and user transparency should be prioritized to increase trust and accountability. Future AI systems should embed explainable AI components that allow end-users, moderators, and investigators to understand the reasoning behind flagged content or coordinated accounts. This not only supports better decision-making but also enables users to contest erroneous classifications, fostering a more open and democratic digital environment.

On the organizational side, the development of interoperable frameworks for cross-platform threat intelligence sharing will be crucial. Coordinated attacks rarely confine themselves to a single platform. The future of CIA detection will likely involve decentralized, collaborative models in which platforms, regulators, researchers, and

civil society organizations share anonymized insights while respecting privacy and security standards. Blockchain and federated learning approaches may play a role in achieving this balance.

There is also growing interest in the application of reinforcement learning and adversarial training to simulate attacker behavior. By modeling how malicious actors adapt to detection, AI systems can be trained in virtual environments to anticipate new tactics. This proactive approach could significantly enhance the resilience of detection mechanisms.

Finally, ethical frameworks and policy integration must evolve in tandem with technological progress. AI developers, legal experts, and human rights organizations must work together to define clear standards for the responsible use of AI in information security. This includes the creation of transparency mandates, impact assessments, and mechanisms for redress in cases of algorithmic harm.

Conclusions. Coordinated information attacks represent a significant threat to modern societies, exploiting the open nature of online communication. AI mechanisms provide powerful tools for detecting and mitigating these threats, leveraging ML, DL, and NLP techniques to uncover coordination and deception. While current methods show promise, continuous research, interdisciplinary collaboration, and ethical considerations are essential to enhance the effectiveness and fairness of AI-driven detection systems.

References

1. Ferrara, E., et al. (2016). “The Rise of Social Bots.” Communications of the ACM.

2. Shu, K., et al. (2020). “Combating Disinformation in a Social Media Age.” ACM SIGKDD Explorations Newsletter.

3. Zhou, X., & Zafarani, R. (2019). “Network-based Fake News Detection: A Survey.” ACM Computing Surveys.

4. Baines, P. R., & O’Shaughnessy, N. J. (2020). “The Dark Side of Political Marketing.” Journal of Public Affairs.

5. Vosoughi, S., Roy, D., & Aral, S. (2018). “The Spread of True and False News Online.” Science.

6. Pennycook, G., & Rand, D. G. (2019). “Fighting misinformation on social media using crowdsourced judgments of news source quality.” PNAS.

7. Ribeiro, M. H., et al. (2020). “Detecting and Characterizing Coordinated Behavior on Social Media.” ICWSM.

8. Jiang, M., et al. (2020). “Political Polarization Drives Online News Consumption: Evidence from COVID-19.” PNAS.

9. Buntain, C., & Golbeck, J. (2017). “Automatically Identifying Fake News in Popular Twitter Threads.” IEEE International Conference on Smart Cloud.