DOI: https://doi.org/10.30525/978-9934-26-500-6-8

Hanna Yarovenko
Doctor of Economic Sciences, Associate Professor,
Associate Professor at the Department of Economic Cybernetics
Sumy State University

DIGITAL TRANSFORMATION: ECONOMY DEVELOPMENT AND FIGHTING AGAINST ILLEGAL PRACTICES[1]

Summary

This study examines the digital transformation of national economies, focusing on key directions, challenges, and prospects, as well as the associated risks of corruption, shadow operations, and cybersecurity threats. Digital transformation is reshaping production, services, and governance by integrating advanced technologies such as artificial intelligence, blockchain, IoT, and cloud computing. These innovations drive efficiency and foster sustainable development yet introduce challenges like unequal access to technology, job displacement, and heightened vulnerabilities to cyber threats. The study highlights the risks linked to corruption and shadow economies that emerge from digitalisation. Misuse of digital platforms, manipulation of algorithms, and lack of transparency in electronic systems facilitate new forms of financial crime and inefficiencies. However, technologies such as blockchain, open data, and automated systems offer solutions for enhancing transparency, automating governance, and reducing human interference. The analysis also delves into the specific risks of digital transformation during wartime, as seen in Ukraine. Issues such as cyberattacks on critical infrastructure, destruction of communication systems, and limited access to resources are compounded by the challenges of maintaining digital governance and economic stability. The study proposes strategies to address these challenges, including decentralised infrastructures, robust cybersecurity measures, and international collaboration. Digital transformation presents both risks and opportunities, demanding a balanced approach to maximise socio-economic benefits while mitigating potential threats.

Introduction

Industry 4.0, which began to develop at the beginning of the 21st century, has led to significant changes in production processes, with modern digital

[1] The work was carried out within the framework of the scientific research № 0124U000544 “Cybersecurity and digital transformations of the country's wartime economy: the fight against cybercrime, corruption and the shadow sector”

technologies such as the Internet of Things (IoT), artificial intelligence (AI), big data, robotics and automation. Its main goal is to increase the efficiency and flexibility of production systems by integrating physical and digital objects, which reduces costs and optimises production processes.

However, the development of Industry 4.0 has also caused certain social and economic consequences. On the one hand, automation and the use of robots have contributed to increased productivity and reduced production costs, which has positively impacted the competitiveness of enterprises. On the other hand, risks have emerged for traditional jobs, as many operations have been automated, which has reduced the number of jobs for unskilled workers. In addition, new challenges have arisen in cybersecurity, as the interconnectedness of systems increases vulnerability to cyber threats [1].

Industry 5.0, which is an evolution of Industry 4.0, focuses on the integration of humans and technology at a new level, increasing the importance of individual needs and the creative potential of workers. This paradigm assumes a more active role of humans in automation processes, where robots and machines function as assistants rather than as a complete replacement for human labour. One of the main directions is the development of personalised production, which allows the creation of products according to individual consumer orders using adaptive production lines and highly developed technologies [1].

At the same time, Industry 5.0 has challenges, among which ensuring the ethics of using artificial intelligence and preserving human dignity in automation conditions is important. The risks associated with the automation of creative professions also require attention, as there is a potential for changes in the labour market, which may lead to new forms of inequality [2].

In addition, Industry 5.0 has a significant environmental dimension. The introduction of more efficient technologies and the transition to sustainable development at the level of enterprises and societies contribute to reducing the negative impact on the environment. The use of renewable energy sources and the development of technologies to reduce carbon emissions is becoming one of the main tasks within the framework of this stage of industrialisation [1].

Therefore, Industry 4.0 and 5.0 create new opportunities for the development of economies but also require a comprehensive approach to solving related problems, such as changing the nature of work, ethical issues and environmental challenges. The successful integration of these technologies requires active cooperation between governments, businesses and society to ensure sustainable and inclusive development in the context of technological transformation.

Digital transformations, which have become a direct consequence of the development of Industry 4.0 and 5.0, mean fundamental changes in the ways of functioning of organisations, business processes and social interactions

through the integration of digital technologies. These transformations cover a wide range of areas, including industry, education, healthcare, finance and government.

In the context of digital transformations, the restructuring of business models is important, which is taking place due to the introduction of the latest digital technologies. For example, the use of cloud computing, artificial intelligence, the Internet of Things and blockchain allows enterprises to create innovative services, optimise processes and provide a personalised approach to consumers. Such an approach provides increased efficiency and competitiveness, contributing to rapid adaptation to changes in the external environment.

Digital transformations also involve a transition from traditional to interactive models of interaction with customers and partners. For example, e-commerce and the use of a blockchain-based "smart" contract platform create opportunities for secure and fast communication between market participants. In industry, this is manifested through the concept of "smart factories", where all elements of the production process are interconnected into a single digital ecosystem.

Education and healthcare have also become important areas of digital transformation. In education, distance learning platforms and adaptive learning systems provide access to quality knowledge regardless of location. In healthcare, the widespread use of digital technologies, such as telemedicine and digital diagnostics, allows to improve the quality of service provision and reduce the cost of healthcare.

Education and healthcare have also become important areas of digital transformation. In education, distance platforms and adaptive learning systems provide access to quality knowledge regardless of location. In healthcare, the widespread use of digital technologies, such as telemedicine and digital diagnostics, allows to improve the quality of service provision and reduce the cost of healthcare.

The changes caused by digital transformations have important social consequences. On the one hand, they contribute to increased productivity and innovation, improving the quality of life. On the other hand, they create new challenges related to uneven access to digital technologies, cybersecurity and privacy. The lack of equal access to digital resources can increase socio-economic inequality between developed and developing countries [1].

Thus, digital transformations are a complex and multifaceted phenomenon that covers all aspects of modern life. They require careful planning and a considered approach to their implementation to ensure maximum socio-economic benefits and minimise potential risks. Industries 4.0 and 5.0 have played a key role in accelerating these changes, providing society with new tools to address modern challenges and build a sustainable future.

Chapter 1. Digital transformation of the country's economy: directions, challenges and prospects

The digital transformation of the economy is a multifaceted process that covers a wide range of areas aimed at increasing production efficiency, expanding access to services and developing innovations. This process is shaping a new economic reality where knowledge, data and technology are key factors. The main areas of the digital transformation of the economy of countries include the following:

1. Development of digital infrastructure. Effective digital transformation is impossible without a highly developed infrastructure that provides fast and reliable access to digital services. The expansion of 5G networks, the development of data centres, satellite Internet and big data storage and processing systems are priorities for many countries. Digital infrastructure is the basis for integrating technologies into production and social processes, as well as for the formation of "smart" cities and regions [3].

2. Digitalization of industry and the agro-industrial complex. In industry, digital transformation is implemented through the concepts of "smart factories" and automation of production processes. This includes the introduction of the Internet of Things, artificial intelligence, additive manufacturing (3D printing) and robotics. The agro-industrial sector is developing "smart farms" that use drones, sensors and analytics to optimise the processes of growing, harvesting and preserving products [3].

3. Digitalization of the financial sector. Financial technologies (fintech) play a key role in the digital transformation of the economy. The introduction of blockchain, mobile payment systems, electronic wallets and automated platforms for asset management creates new opportunities for consumers and businesses. Digital currencies, in particular central bank digital currencies (CBDCs), are becoming an important tool for modernising countries' financial systems [4; 5].

4. E-government and digital public services. The digitalisation of public administration involves the creation of platforms for the provision of electronic services, such as business registration, tax payment, receiving social assistance, etc. The development of open data systems, as well as the use of blockchain and artificial intelligence technologies in decision-making, contribute to increasing the transparency and efficiency of public administration [3].

5. Development of e-commerce and digital markets. E-commerce is one of the most dynamic areas of digital transformation. Online trading platforms, marketplaces and electronic platforms for small and medium-sized businesses contribute to the globalisation of economic activity. Thanks to this, even small companies can enter international markets [4; 5].

6. Investing in education and the development of digital skills. Successful digital transformation of the economy requires qualified personnel. States are

investing in the development of digital skills of the population through the modernisation of educational programs and the creation of innovation centres and training platforms. Particular attention is paid to the training of specialists in the fields of AI, data analysis, cybersecurity and programming [3].

7. Development of a "green" economy through digital technologies. Digital transformation supports sustainable development through the introduction of innovations in the field of energy, environmental monitoring and resource management. "Smart" energy grids, pollution monitoring systems and waste management technologies contribute to reducing the environmental burden on the planet [3].

8. Expanding digital rights and ensuring cybersecurity. Data protection, combating cybercrime and ensuring the privacy of citizens are becoming key tasks for countries implementing digital transformation. Regulatory initiatives and the introduction of new security standards are important components of the digitalisation strategy [6].

The digital transformation of the economies of countries is a multidimensional process that contributes to increased economic efficiency, social inclusion and sustainable development. At the same time, success in this area depends on a comprehensive approach that includes investments in infrastructure, human capital, innovation and ensuring an appropriate regulatory environment.

The development of digital technologies has significantly increased the dependence of countries on information systems and digital infrastructure. In this regard, ensuring cybersecurity has become one of the strategic directions of transformation, which aims to protect economic, social and political systems from threats associated with cybercrime, espionage, sabotage and other forms of cyberattacks.

Cybersecurity requires a systemic approach, which is implemented through the adoption of national strategies that define key policy directions, coordination mechanisms between government structures and the private sector, as well as the main goals in the field of information systems protection. Such strategies consider the development of a regulatory framework, the creation of institutions for monitoring and countering cyber threats, as well as the implementation of international cyber defence standards.

The digitalisation of critical infrastructure, including energy systems, transport, financial institutions and public services, creates potential risks due to the possibility of their destabilisation due to cyber attacks. To ensure the smooth operation of these sectors, it is important to [7]:

– use of real-time cyber threat monitoring tools;
– backup of data and key infrastructure components;
– conduct regular security audits and vulnerability testing, including cyber attack simulation.

Modern cyber defence systems include integrated monitoring platforms that can identify and respond to potential threats before they cause significant damage. The use of artificial intelligence and machine learning technologies allows for analysing anomalies in data traffic and detecting suspicious activity. Computer Emergency Response Teams (CERTs) are being established at the national level to coordinate measures to address cyber threats [7].

Legal regulation of cybersecurity is an integral part of digital transformation. Key aspects include:

– implementing legislation that obliges companies to protect user data and report cyber incidents;

– creating framework agreements for the exchange of information between states and private organisations;

– ensuring accountability for cyberattacks, including international cooperation in investigating cybercrimes.

The human factor remains one of the weakest points in cybersecurity. Therefore, the development of education in this area is key. Measures include:

– conducting training programs for critical infrastructure workers;

– informing citizens about basic rules of digital hygiene, in particular password protection, caution in using emails and social networks;

– creating specialised educational institutions and courses to train cybersecurity experts.

Given the global nature of cyber threats, international cooperation is an important element of cyber defence. Countries conclude agreements on information exchange, develop joint incident response protocols and participate in international cyber defence exercises. Organisations such as NATO, the United Nations and the European Union develop standards and recommendations to ensure cybersecurity at the global level [7].

Innovation plays a central role in countering new cyber threats. The main directions are [3]:

– use of blockchain to ensure transaction security and authentication;

– implementation of biometric systems for user identification;

– development of quantum cryptography to increase the security of advanced data transmission systems.

Preserving the privacy of citizens in the digital environment is an important aspect of cybersecurity. The implementation of standards such as the General Data Protection Regulation (GDPR) in EU countries serves as an example of a comprehensive approach to information protection.

Thus, cybersecurity is one of the key areas of digital transformation, as it ensures the stability of the digital economy, the protection of critical infrastructure and the rights of citizens. Investments in cyber defence, the development of the regulatory framework, public education and international

cooperation are prerequisites for the successful resolution of modern challenges in the field of cybersecurity.

Digital transformations play an important role in the development of the economy, public administration and public life. However, for countries in a state of war, this process is accompanied by numerous problems caused by the specific challenges of wartime. War increases the vulnerability of digital systems, changes the priorities of state policy and complicates the implementation of long-term transformation strategies.

During the war, critical digital infrastructure becomes the target of targeted attacks. This includes:

– cyberattacks on government, military, and financial systems. The aggressor can use cyberattacks to destabilise the government, disrupt the functioning of the banking system, and create chaos in society;

– physical destruction of telecommunications infrastructure. The destruction of data centres, fibre optic lines, and mobile towers significantly complicates the maintenance of communications;

– difficulties in ensuring cybersecurity. In conditions of constant external pressure, resources may be insufficient to respond to a wide range of cyber threats.

Military actions lead to the emigration of qualified specialists, particularly from the IT sector. The loss of human capital complicates the implementation of digital innovations, the development of high-tech industries, and the maintenance of already-created systems.

During times of war, resources are directed primarily to ensuring the country's defence capabilities, which often puts digital transformations on the back burner. Key aspects include:

– redirection of budget funds to military needs, which reduces opportunities for investment in digital infrastructure;

– focusing on operational needs, such as the introduction of military technologies, to the detriment of long-term civilian projects.

Countries at war often face economic sanctions, logistical difficulties, and destruction of infrastructure, which complicates access to modern technologies and materials for their implementation. Ensuring the functioning of the digital economy can be complicated by shortages of equipment, software, and services.

War deepens the digital divide between different population groups. In areas that have suffered destruction, access to the Internet and electronic services can be completely lost. At the same time, in peaceful regions, the level of digitalisation can continue to grow, which creates new forms of inequality.

In the wars of the 21st century, digital technologies are becoming an important tool of aggression. The main threats include:

– disinformation and information attacks. The massive spread of fake news destabilises society, influences public opinion and undermines trust in state institutions;

– cyber espionage. Hacking of state databases and infrastructure to obtain confidential information about the country's military or economic plans.

The economic consequences of war, including a decline in production, reduced investment and loss of tax revenues, limit the ability of the state and businesses to finance digital projects. Small and medium-sized enterprises, which are the drivers of digital transformation, may lose access to markets and resources.

War creates psychological pressure on society, reducing motivation to learn, innovate and implement new technologies. Society may experience an increase in distrust of digital tools due to fear of cyber threats and information manipulation.

Despite these challenges, countries can implement strategies to minimise the negative impact of war on digital transformation:

1) decentralizing infrastructure through the use of cloud technologies and satellite internet to ensure resilience to physical destruction;

2) strengthening cybersecurity by expanding international cooperation and using artificial intelligence to counter threats;

3) supporting human capital, including distance learning programs and encouraging the return of emigrants;

4) mobilizing international assistance to restore infrastructure and ensure access to critical technologies.

War thus creates significant obstacles to digital transformation, but it also stimulates the search for innovative solutions to adapt to new realities. Countries in a state of war must combine strategies to respond to current challenges with long-term planning for digital transformation aimed at recovery and development in the post-conflict period.

Ukraine's digital transformation, which is actively developing even in times of war, faces some problems related to military aggression and difficult socio-economic circumstances.

The following challenges it faces can be identified:

1. Cyber threats. Constant attacks on Ukraine's critical infrastructure, including energy, financial, and government systems, significantly complicate the implementation of digital technologies. For example, in 2022–2023, the intensity of cyber attacks was unprecedented, which forced Ukraine to seek support from international partners to create backup data centres abroad (for example, in Poland) to store data and ensure the stable operation of digital services such as "Diya" [8; 9].

2. Migration and staff shortage. The war caused a significant outflow of IT specialists abroad, in particular to Poland, the Czech Republic, and other

countries. According to the IT Research Ukraine 2023 study, many companies are forced to open offices abroad, which reduces the local potential for digital innovation [8; 9].

3. Financial support for startups. In times of war, innovative projects face funding challenges and high risks. Grant funding programs have been launched to support startups, such as Brave1 for defence technologies. However, the scale of support does not yet match the needs, and many startups are suspending development or reorienting to international markets [8; 9].

4. Destroyed infrastructure. A significant amount of communication and technical infrastructure has been damaged due to hostilities. Recovery programs such as eRecovery have already contributed to housing repairs and IT infrastructure upgrades, but the process remains complex and lengthy [8; 9].

Although Ukraine has demonstrated adaptability and a high level of resilience, the challenges of the war significantly slow down the pace of digital transformation. To address them, it is important to maintain and develop international support, expand access to financing, and maintain a focus on strategic areas such as cybersecurity and the development of defence technologies.

But despite the challenges that may arise from wars and cyber threats, digital transformation is one of the key factors that will shape the economic development of countries in the coming decades. Given the rapid development of technologies, the future of the digital economy promises significant changes that can significantly change the nature of production processes, the structure of labour markets and business models. In this context, several important prospects and trends can be identified [2].

1. Integration of artificial intelligence and automation. AI and automation are becoming the main drivers of the development of digital transformations. According to forecasts, by 2030, most industries, including manufacturing, transportation, medicine and financial services, will implement AI to optimize processes, increase efficiency and reduce costs. For example, automation of production allows not only to reduce labour costs but also to ensure high accuracy and stability in the work of enterprises. Countries that actively implement these technologies will have significant competitive advantages in the global market [10].

2. Development of digital currencies and blockchain technologies. Digital currencies and blockchain will continue to transform economic systems. Governments and central banks are exploring the possibility of introducing central bank digital currencies (CBDCs), which can simplify payments, reduce transaction costs and improve the transparency of financial transactions. On the other hand, blockchain is becoming the basis for the development of secure and transparent supply chains, where countries that implement these technologies

will be able to achieve significant economic benefits, reducing corruption and increasing trust in economic processes [11].

3. Development of the Internet of Things (IoT) and "smart" cities. The Internet of Things, which involves connecting physical objects to the Internet, will provide new opportunities for the efficient use of resources. In the future, "smart" cities with integrated IoT systems will help reduce pollution, reduce energy costs and improve the quality of life. Countries that actively develop IoT infrastructure can create more resilient economic systems that can adapt quickly to changes and challenges in the global economy [12].

4. Accelerated 5G and mobile technology development. With the introduction of 5G networks, countries will gain new opportunities for the development of digital services, including high-speed mobile communications, remote control and new technologies for industry. This will contribute to the development of sectors such as healthcare, transport and logistics, and will open new opportunities for startups and small businesses in the digital environment [7].

5. Transition to digital platforms and new business models. Digital platforms continue to transform countries' economic models, including in the services sector, retail, finance and manufacturing. The transition to a platform as a business model allows countries to adapt more quickly to changing demand and global trends. At the same time, it creates new opportunities for micro and small-scale enterprises, which contribute to economic development and job creation. However, countries that do not invest in the development of infrastructure for such platforms may fall behind others in the digital competition [10].

6. Challenges for cybersecurity and data protection. Digital transformation is growing along with new cybersecurity threats. Governments and companies must invest in data protection and ensure the security of digital systems. The threat of cyberattacks and hacking of personal and financial data is a serious problem that requires national cybersecurity strategies. Countries that can adequately protect their digital infrastructure will have important advantages in the global economy [10].

7. Environmental aspect of digital transformation. The transition to digital technologies has an impact on the environment, through the energy consumption of data centres and the production of hardware. In the future, many countries will focus on the sustainable development of digital technologies, using "green" technologies and renewable energy sources to support their digital infrastructure. This will become an important component of the global economic development strategy [6].

The future of digital transformation promises significant economic benefits for countries that can effectively use the latest technologies, integrate innovations across sectors of the economy, and create resilient and adaptive

digital infrastructures. At the same time, these processes will require governments to invest significantly in infrastructure development, education, and cybersecurity.

Chapter 2. Corruption, shadow operations, money laundering and cyber threats: risks and potential of digital transformations

Digital transformations can create conditions for new forms of corruption. The integration of digital technologies into government and economic systems can generate risks related to the misuse of digital tools, insufficient regulation and uneven levels of digital literacy. What risks can be generated for the spread of corruption?

1. Misuse of digital platforms. Digital platforms created to ensure transparency can become objects of manipulation. Imperfect system design or weak access controls can allow individuals or groups to change data in registries, manipulate algorithms or influence the allocation of resources. For example, e-procurement systems, while promoting openness, can be used to create fictitious tenders, which opens new corruption risks [13].

2. Lack of transparency in software algorithms. Automation of processes, particularly the use of artificial intelligence algorithms, can become a source of corruption due to their lack of transparency. Algorithms that make decisions, for example in the processes of distributing finances or determining the winners of tenders, can be manipulated or have hidden biases that are difficult to detect and control. This can increase inequality in access to resources and support corrupt practices [14].

3. Risks of uneven access to digital resources. Inequality in access can create the prerequisites for corruption. Citizens or businesses that do not have sufficient skills or resources to work with digital platforms may be forced to turn to intermediaries, who can often use their position to illegally gain benefits or influence the outcomes of processes.

4. Cyber threats. Insufficient cybersecurity in digital systems opens opportunities for abuses such as data theft, information forgery or the use of confidential data for blackmail. In the field of public administration, attacks on electronic platforms can be aimed at falsifying data, which undermines trust in digital transformations and contributes to new forms of corruption.

5. Lack of regulatory control. Digital technologies often develop faster than the corresponding legal and ethical norms emerge. The lack of adequate regulation can allow unscrupulous users to exploit digital platforms for their interests. For example, in the field of cryptocurrencies and digital assets, unregulated transactions can be used for money laundering and tax evasion [13].

6. Risks in the field of personal data. Inadequate management of personal data can create opportunities for the misuse of information for the purpose of

obtaining illicit benefits. Public registries and electronic data storage systems become targets of attacks and manipulation if their protection is insufficient, which opens the way for new forms of corrupt activities.

Digital transformations can become a new source of risks if their implementation is not accompanied by appropriate control and security measures. To minimize such risks, it is necessary to introduce clear regulatory mechanisms, ensure transparency of digital platforms, increase the digital literacy of citizens and strengthen cybersecurity. Only under these conditions will digital innovations be able to realize their potential in combating corruption. They open wide opportunities for combating corruption by increasing transparency, reducing the human factor in decision-making and automating management processes. The effectiveness of digital technologies in this context is confirmed by numerous examples both at the international level and in Ukraine. Let us consider potential areas of their use to combat corruption.

1. Use of electronic platforms and transparency of public services. Digitalization of public services allows to reduce corruption risks by eliminating direct contact between citizens and officials. For example, in Ukraine, the "Diya" platform already provides a wide range of online services, which significantly reduces opportunities for corruption abuses. For example, automating the procedures for obtaining licenses, registering a business, and processing social assistance provides transparency and simplicity, eliminating opaque "deals" [15].

2. Open data and public control. Open data is a key tool for monitoring public procurement, the budget, and the activities of officials [15]. For example, the ProZorro system in Ukraine has significantly reduced corruption in public procurement due to public access to information about tenders. According to research, the use of ProZorro has saved the state billions of hryvnias and increased trust in the procurement process [16].

3. Blockchain as a means of combating corruption. Blockchain technologies create the opportunity to maintain transparent and immutable records of financial transactions, state property, and other assets. Its use in land cadastres or property rights registers significantly reduces the risk of fraud and corruption schemes. For example, Ukraine is working on implementing blockchain solutions in the registration sphere to eliminate the possibility of document manipulation and reduce the time for checking information [11].

4. Electronic tenders and automation of budget control. Automated budget allocation systems based on algorithms and clear rules minimize the risk of manual intervention in processes. For example, Ukraine has an electronic declaration system for officials that allows them to track their income and expenses. Artificial intelligence-based analytics tools can be used to detect suspicious transactions or discrepancies in financial data [15].

Despite the significant potential of digital transformations, many challenges need to be addressed to achieve the full effect. Key issues include:

– the technological gap between regions, which complicates citizens' access to digital services;

– data security, as digitalization increases the risks of data leakage and cyberattacks;

– "resistance to change", which is often found on the part of corrupt structures or outdated management systems.

Digital transformations are a powerful tool for combating corruption through increased transparency, process automation and the introduction of innovative technologies such as blockchain and open data. At the same time, effective digitalization requires institutional support, citizen education and an adequate level of data protection to avoid new threats and ensure the sustainable development of anti-corruption mechanisms.

The use of digital tools in the shadow economy creates new challenges. Thus, the development of digital platforms, e-commerce and cryptocurrencies creates risks that can stimulate illegal activities and complicate the control of financial flows. This can manifest itself in the following types of risks.

1. Use of cryptocurrencies for anonymous transactions. Cryptocurrencies such as Bitcoin, Ethereum and others provide a high level of anonymity for financial transactions. This makes them attractive for shadow operations, including tax evasion, criminal financing and money laundering. The lack of centralized control over cryptocurrency transactions makes them difficult to monitor and creates favourable conditions for abuse [4; 5].

2. Shadow e-commerce. E-commerce platforms can be used to sell illegal goods and services, such as forged documents, counterfeit products or prohibited substances. In particular, the Darknet is home to numerous online marketplaces where transactions are made using anonymous payment methods, such as cryptocurrencies, which makes them difficult to track.

3. Use of digital platforms for fraud. Digital platforms that facilitate access to financial and trading services can be used for fraudulent schemes. For example, crowdfunding or e-commerce platforms are sometimes used to raise funds for fictitious projects, which contributes to the development of fraud in the digital sphere [4; 5].

4. Abuse of electronic payment systems. Electronic wallets and payment systems such as PayPal, Revolut and others provide convenience for transactions but also pose risks. These services can be used to transfer money while concealing the origin of the funds. For example, in Ukraine, such tools are often used to circumvent tax regulations or shift income into the shadow economy [4; 5].

5. Darknet and the digital transformation of criminal activity. The development of anonymous networks such as Tor provides the shadow

sector with tools to conduct illegal operations with a high degree of protection from detection. This is especially true in areas such as arms, drugs or even human organ trafficking. Digital transformations make it more difficult to combat such activities due to the speed of information exchange and the difficulty of monitoring encrypted data.

6. Illegal use of Big Data. Big data analysis systems, which are critical to the digital economy, can also be used in shadow operations. In particular, criminals can use them to create complex tax evasion schemes, manipulate financial markets or prepare for cybercrime [17].

On the one hand, digital transformations contribute to the globalization and convenience of financial transactions, but on the other hand, they also create new risks for the growth of the shadow economy. To counter these challenges, it is necessary to strengthen regulatory oversight, increase the transparency of digital platforms, and develop international cooperation in the field of monitoring illegal activities. The effective use of digital tools to combat shadow transactions is an important step towards creating a safe and transparent digital economy.

The shadow economy poses a significant challenge for countries, reducing tax revenues, reducing trust in state institutions and hampering economic development. Digital transformations open new opportunities to combat shadow operations by increasing transparency, automating financial processes and improving monitoring systems. How can the potential of technology be used to combat the shadow economy?

1. Digitalization of financial transactions. The use of non-cash payments contributes to the reduction of cash payments, which are often the basis of the shadow economy. For example, in Ukraine, the popularity of digital payment platforms is growing, which allows recording all transactions, reducing opportunities for tax evasion [4; 5].

2. Introduction of digital currencies. Central bank digital currencies have the potential to significantly reduce the shadow economy. They allow for control over the movement of money and the detection of illegal financial transactions. For example, several countries, including Ukraine, are considering the introduction of digital currencies to increase the transparency of economic activity and combat money laundering.

3. Use of big data and artificial intelligence. Big data analytics and artificial intelligence provide a new level of detection of shadow transactions. AI-based systems can analyse large volumes of transactions, identifying anomalies that indicate illegal activity. For example, Ukraine is implementing analytical systems for the automatic detection of fraudulent schemes in the tax sphere, which allows for an increase in the efficiency of monitoring financial transactions [17].

4. Automation of tax systems. Electronic tax administration is an effective means of combating shadow transactions. Automated tax systems reduce the risk of human error or manipulation by employees, which provides better control over tax payments. Ukraine has successfully implemented an electronic tax invoice system, which has significantly reduced the level of tax abuse.

5. Blockchain technologies. Such technologies offer a decentralized and transparent system of recording transactions, which makes it impossible to change them without a trace. Blockchain can be used to control supply chains, monitor government procurement and detect shady schemes. In the future, its implementation can become a standard in financial reporting and prevent tax evasion [11].

6. Electronic registries and open information. Electronic registries of real estate, businesses and other assets to ensure transparency of ownership and avoid illegal use of assets. For example, in Ukraine, a number of electronic registries are already in operation, such as the Real Estate Registry, which helps to combat shady transactions in this area.

Digital transformation is a powerful tool for combating shadow transactions. The use of modern technologies, such as digital currencies, blockchain and artificial intelligence, can significantly increase the effectiveness of the fight against illegal economic activities. At the same time, the success of these initiatives depends on a systemic approach, the development of appropriate infrastructure and the protection of personal data. They also open up new opportunities for financial transactions, but at the same time make it difficult to control the flows of illegally obtained funds. Innovative digital tools, such as cryptocurrencies, decentralized financial services and electronic payment platforms, are becoming increasingly popular among criminals to legalize proceeds from crime. What risks can innovative technologies generate?

1. The use of cryptocurrencies in money laundering schemes. Cryptocurrencies provide a high degree of anonymity, which makes it difficult to trace the origin of funds. Criminals use cryptocurrency mixers, exchangers or “dark” wallets to disguise financial flows. In many cases, such transactions evade regulation, allowing criminals to effectively hide their sources of income [4; 5].

2. Decentralized Financial Services (DeFi). The DeFi sector, which provides lending, asset exchange, and other financial transactions without involving intermediaries, is becoming an important tool for money laundering. The lack of centralized management and regulatory oversight allows for complex financial transactions that are difficult to control or track. For example, criminals can transfer funds across different decentralised platforms, using smart contracts to obfuscate the traces of transactions [4; 5].

3. Abuse of electronic payment platforms. Electronic wallets and payment services such as PayPal or other digital platforms provide speed and

convenience for financial transactions but, at the same time, open opportunities to hide illegal transactions. Although many of these platforms have monitoring systems, their effectiveness may be limited by the high volume of transactions and the lack of a unified approach to regulation.

4. Money laundering through online gambling. Online betting and casino platforms create a convenient environment for the legalisation of criminal proceeds. Criminals use these services to deposit illegal funds, place bets, and withdraw winnings that formally look like legal profits. In some countries, including Ukraine, the regulation of online gambling is still at the development stage, which creates additional risks and stimulates the legalisation of criminal proceeds.

5. Use of the Darknet for financial manipulation. The Darknet, as a tool for shadow operations, is becoming an important channel for money laundering. Using anonymous transactions and cryptocurrencies, criminals can make transfers without leaving a digital trace. Many darknet platforms are integrated with crypto exchanges, making it more difficult to combat illicit financial flows.

6. Risks in the context of international transactions. The growth of international financial transactions through digital platforms creates additional challenges. The lack of harmonised rules for monitoring such transactions between countries allows criminals to move funds through jurisdictions with a low level of regulation. This contributes to the formation of global money laundering schemes [4; 5].

The digitalisation of the financial sector creates serious challenges for combating money laundering. To minimise these risks, it is necessary to improve regulatory mechanisms, ensure transaction transparency, increase cooperation between countries and implement technological solutions for automatic monitoring of financial flows. These measures are important for creating a reliable system of financial security in the context of digital transformation.

Modern computer technologies create a wide range of opportunities for detecting, preventing and combating the legalisation of criminal proceeds. They increase the effectiveness of monitoring financial transactions, automate risk analysis processes and strengthen control over suspicious transactions. That is why digital transformations have the corresponding potential to reduce the risks of money laundering. What areas can be identified here?

1. Digital monitoring of financial flows. The use of digital technologies in the financial sector allows for continuous monitoring of transactions. Analytical systems integrated with banking platforms can automatically detect suspicious transactions according to established algorithms. Standards such as Know Your Customer (KYC) and Anti-Money Laundering (AML), which are based on digital verification of the identity of customers and analysis of their

financial behaviour, are already being used in the world. In Ukraine, in particular, banking institutions are implementing transaction monitoring systems based on artificial intelligence, which allows them to identify suspicious activity and block potentially illegal operations.

2. Blockchain technologies for transaction transparency. Blockchain is an important tool in the fight against money laundering due to its immutability and transparency. All transactions recorded in the blockchain registry cannot be changed or deleted, which creates an open and immutable trail of financial activity. The use of blockchain in financial reporting and property registries significantly reduces the risks of concealing sources of income. For example, Ukraine is implementing blockchain for monitoring state assets, which can also be adapted to control illegal financial flows [11].

3. Artificial intelligence and big data analysis. They provide effective analysis of large volumes of financial data, allowing to quickly identify risks. AI algorithms can analyse transactions in real time, detecting anomalies that may indicate money laundering. For example, AI-powered financial flow analysis allows banks and financial regulators to track complex money laundering schemes [17].

4. Identity verification through digital identifiers. Digital identifiers provide transparency in verifying the identity of customers. Biometric authentication tools, electronic signatures, and other technologies help prevent document forgery and the creation of shell companies, which are often used to launder money.

5. Integration of international databases. Digital transformations are facilitating the integration of national databases with international systems, making it much more difficult to use cross-border money laundering schemes. Ukraine, for example, is working with international organisations such as the Financial Action Task Force (FATF) to implement financial monitoring standards and use global databases to verify transactions and counterparties.

6. Electronic reporting platforms. Their implementation for financial reporting promotes transparency of companies' activities and reduces the possibility of income concealment. Electronic declarations and platforms for automatic exchange of financial information allow for more effective monitoring of the activities of companies and individuals involved in suspicious financial transactions.

Digital transformations have significant potential in countering money laundering through transparency of financial processes, data integration and automation of risk detection. Effective use of technologies such as blockchain, artificial intelligence and digital identifiers can minimise money laundering risks and enhance trust in financial systems. However, to realise this potential, it is necessary to strengthen international cooperation, develop national digital

infrastructure and improve the skills of specialists in the field of financial monitoring.

Although the rapid development of digital transformations significantly increases the efficiency of economic and social processes, it also contributes to the expansion of the spectrum of cyber threats. The integration of new technologies, such as artificial intelligence, the Internet of Things (IoT) and cloud computing, creates new vulnerabilities that can be used by attackers. What risks from digitalisation can lead to the possibility of cyber threats?

1. Increasing complexity of cyber attacks. The expansion of digital infrastructure increases the complexity and scale of cyber attacks. Attackers use artificial intelligence to automate attacks and increase their efficiency and complexity. For example, so-called Deepfake technologies can be used to compromise organisations by forging the voice or images of managers, which creates risks of financial losses and information sabotage [7].

2. Vulnerabilities of the Internet of Things. IoT devices, which are actively implemented in various sectors of the economy, are one of the main targets for cybercriminals. Due to the low level of protection of these devices (for example, lack of regular software updates or insufficient security protocols), they can be used for mass attacks such as DDoS or for the collection of confidential information [12].

3. Vulnerabilities of cloud systems. The transition to cloud computing as part of digital transformation carries risks associated with data concentration. A security breach in a single cloud infrastructure can lead to a large amount of information leakage. Attackers can exploit insufficiently protected cloud environments to steal data, blackmail, or sabotage systems [18].

4. Digital attacks on critical infrastructure. The expansion of digitalisation of critical infrastructure, including energy, transportation, and the financial system, increases their vulnerability to cyber threats. Attacks on these objects can have large-scale socio-economic consequences. For example, the 2015 attack on Ukraine's power grid demonstrated how digital vulnerabilities can be used to exert large-scale influence over a state [7; 19].

5. Social engineering risks. Digital transformations are making it easier to access personal data, which makes social engineering techniques more effective. Hackers are using open-source information to create personalised phishing attacks that are difficult to recognise, even for experienced users [20].

6. Illegal use of big data. Big data analysis is becoming a critical tool for the digital economy, but it can also be used for cybercrime. For example, attackers can use algorithms to identify vulnerabilities in financial systems or create personalised attacks based on users' behavioural data [17].

Digital transformations significantly expand the range of cyber threats, especially in areas where information is a key asset. To reduce risks, it is necessary to implement comprehensive cybersecurity strategies that include

strengthening the protection of digital infrastructure, increasing user awareness, developing a regulatory framework and international cooperation. This will minimise threats and ensure the sustainable development of the digital economy in the face of global challenges. The potential of digital technologies allows us to improve cybersecurity mechanisms, not only by protecting critical infrastructure but also by preventing new types of attacks using innovative technologies. This becomes possible in the following areas.

1. Artificial intelligence for detecting and preventing threats. Artificial intelligence and machine learning are effective tools for detecting anomalies in digital systems. Their algorithms can analyse large amounts of data in real time, identifying suspicious activity that may indicate a cyberattack. For example, in the field of cyber defence of critical infrastructure of Ukraine, AI-based systems are used that allow to automatically detect threats and respond to them.

2. Use of blockchain technologies. Blockchain offers a high level of security for protecting data and digital transactions. Its decentralised nature and cryptographic security significantly complicate information manipulation or unauthorised access. For example, blockchain can be used to protect state registries and ensure the authenticity of documents, which is especially relevant for Ukraine in the context of military aggression and cyber attacks on state systems [11].

3. Cloud technologies for security. Cloud services integrated with cyber defence solutions allow the provision of data redundancy and protection in case of attacks. The use of distributed cloud platforms also increases the resilience of systems to DDoS (distributed denial of service) attacks [18]. In Ukraine, cloud technologies are actively implemented in the public sector to ensure the continuity of systems in the face of risks associated with war.

4. Internet of Things (IoT) and cybersecurity. The Internet of Things creates new opportunities for digital transformation, but at the same time is a potential vector of attacks. Monitoring systems integrated with the Internet of Things for the timely detection of network weaknesses and block off unauthorised access to devices. In the context of Ukraine's energy security, IoT systems are used to monitor the status of critical infrastructure facilities, minimising the risks of cyberattacks [12].

5. Automation and prediction of attacks. Automated cyber threat analysis systems allow for the prediction of potential attack scenarios and the adoption of preventive measures. Modern cybersecurity platforms are capable of not only detecting but also automatically neutralising malicious programs or suspicious activities before they affect systems. For example, Ukraine is working on integrating early warning systems into government agencies and critical infrastructure enterprises [7].

6. International cooperation and security standards. Digital transformations also contribute to improving international coordination in the field of

cybersecurity. The integration of Ukrainian systems with global standards, such as ISO 27001, as well as information exchange through NATO or EU platforms, helps to effectively respond to modern cyber threats and prevent their consequences [7].

The potential of digital transformations in countering cyber threats is significant due to the integration of innovative technologies, such as AI, blockchain and IoT, which allow for a proactive approach to data and infrastructure protection. However, the realisation of this potential requires significant investments in cybersecurity, the development of digital literacy, as well as international cooperation to create resilient digital ecosystems.

Conclusions

Digital transformations of the economy are an integral part of modern global development, shaping new business models, approaches to government and social interactions. Industries 4.0 and 5.0 play a central role in these changes, integrating automation, artificial intelligence, the Internet of Things and personalised production processes. Industry 4.0 focuses on increasing production efficiency, reducing costs and implementing the latest technologies. In contrast, Industry 5.0 emphasises a humanistic approach, where technology complements humans while maintaining their central role in creative and intellectual processes.

However, digital transformations are accompanied by numerous challenges. The loss of traditional jobs due to automation requires workers to reorient themselves towards new professions and develop digital skills. Cybersecurity threats associated with the integration of technologies into all areas of activity pose risks for both businesses and government structures. Socio-economic inequalities are exacerbated by limited access to technology in less developed regions. In addition, environmental issues remain important, as digital innovations require significant resources and energy.

The success of digital transformations depends on the development of infrastructure, such as 5G, cloud technologies, blockchain and data centres. In industry, concepts of "smart factories" and agricultural technologies play an important role in optimising production processes and contributing to sustainable development. E-government and the development of financial technologies, such as blockchain and digital currencies, are the basis for the modernisation of public services and the transparency of financial transactions.

However, digital transformations also open new risks in the field of corruption, the shadow economy and the legalisation of criminal proceeds. As noted in Chapter 2, the misuse of digital platforms, manipulation of algorithms and unequal access to digital resources create new forms of corruption. For example, electronic tenders can be used to create fictitious

schemes, and insufficient control over cryptocurrencies facilitates anonymous financial transactions. The shadow economy also actively uses innovative tools such as DeFi, online gambling and the darknet, which makes it difficult to detect illegal financial flows.

Despite this, digital tools have significant potential to combat corruption and the shadow economy. The use of open data, transaction monitoring systems, and blockchain provides transparency and automation of processes, minimising the human factor. For example, in Ukraine, the Diia platform and the ProZorro system have already demonstrated effectiveness in reducing corruption in the public sector [16]. The development of international cooperation, the integration of national databases with global systems and the implementation of standards such as GDPR are important components for ensuring the security and transparency of digital processes.

Cybersecurity remains critical for the successful implementation of digital transformations. The growing volume of cyberattacks, vulnerabilities of IoT devices and risks of cloud platforms require a comprehensive approach. Innovations such as artificial intelligence, blockchain, and automated threat analysis systems create opportunities for effective responses to cyber threats. In times of war, as Ukraine's experience shows, data backup, international cooperation in cyber defence, and the implementation of early detection systems are important.

In conclusion, digital transformation is a multifaceted phenomenon that encompasses all aspects of economic, state, and social life. Its successful implementation requires investments in infrastructure, human capital, and cybersecurity, as well as prudent regulation aimed at minimising risks. With a comprehensive approach, digital transformation will become the basis for sustainable development, innovation, and competitiveness of economies on a global scale.

References:

1. Schwab K. (2016). The fourth industrial revolution. Crown Business.
2. WEF. (2020). The future of jobs report. World Economic Forum. Available at: https://www.weforum.org/reports/the-future-of-jobs-report-2020
3. OECD. (2019). Going digital: Shaping policies, improving lives. OECD Publishing. DOI: https://doi.org/10.1787/9789264312012-en
4. International Monetary Fund. (2024). Cyber risk: A growing concern for macrofinancial stability. International Monetary Fund. Available at: https://www.imf.org/en/Publications/GFSR
5. European Central Bank. (2024). Cyber resilience of financial institutions: A growing challenge. European Central Bank. Available at: https://www.ecb.europa.eu/
6. European Commission. (2021). Shaping Europe's digital future. Available at: https://ec.europa.eu/digital-strategy
7. NATO Cooperative Cyber Defence Centre of Excellence. (2022). Cyber security in critical infrastructure: Lessons learned. NATO CCDCOE.

8. National Institute for Strategic Studies (NISS) (2023). Impact of war on digital transformation in Ukraine. NISS Publications.

9. Ministry of Digital Transformation of Ukraine (2023). IT sector challenges during wartime. Government of Ukraine.

10. Brynjolfsson E., McAfee A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W. W. Norton & Company.

11. Tapscott D., Tapscott A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin.

12. Manyika J., Chui M., Bughin J., Dobbs R., Bisson P., Marrs A. (2013). Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute.

13. Fuest C., Plekhanov A. (2017). The role of information technology in combating corruption and money laundering in the financial sector. *Journal of Financial Regulation and Compliance*, vol. 25(1), pp. 1-15. DOI: https://doi.org/10.1108/JFRC-07-2016-0057

14. BigEubanks V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. *St. Martin's Press*, vol. 1(1). DOI: https://doi.org/10.5204/lthj.v1i0.1386

15. Pardo T. A., Lemo, A. (2014). The open government partnership: Promise and risks of its role in reducing corruption. *Journal of Public Administration Research and Theory*, vol. 24(3), pp. 625-634. DOI: https://doi.org/10.1093/jopart/mut048

16. Kelman, S. (2022). Overcoming Corruption and War – Lessons from Ukraine's ProZorro Procurement System. Available at: https://www.hks.harvard.edu/publications/overcoming-corruption-and-war-lessons-ukraines-prozorro-procurement-system

17. Gandomi A., Haider M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management,* vol. 35(2), pp. 137–144. DOI: https://doi.org/10.1016/j.ijinfomgt.2014.10.007

18. McKinsey & Company. (2023). The new role of cybersecurity in financial services. McKinsey & Company. Available at: https://www.mckinsey.com/

19. OECD. (2024). Financial sector cybersecurity: Risks and mitigation. Organisation for Economic Co-operation and Development. Available at: https://www.oecd.org/digital/

20. American Bankers Association. (2024). Seven cybersecurity threats for banks in 2024 – and some smart precautions. American Bankers Association. Available at: https://bankingjournal.aba.com