THE TRANSFORMATION OF ENTREPRENEURIAL ACTIVITY IN THE CONDITIONS OF THE DEVELOPMENT OF THE DIGITAL ECONOMY AND A METHODOLOGY OF ASSESSING ITS DIGITAL SECURITY

Viktoriya GONCHAR
Pryazovskyi State Technical University
University str. 7, 87555, Mariupol, Ukraine
E-mail: gonchar.mariupol@gmail.com
ORCID ID: 0000-0002-8765-6656

***Abstract**. The innovative way that business is developed in the context of the digitalization of the Ukrainian economy dictates conditions where modernization and the development and strengthening of business positions on an international scale become more and more significant and unavoidable for every enterprise. Therefore, this is subject to detailed control and the implementation of digital security. The purpose of this study is to substantiate and develop theoretical and methodological provisions and scientific and practical recommendations for improving the system of businesses' economic security in the digital economy.*
The stages of introduction of digital technologies were considered. This made it possible to trace the chain of development of digitalization in the country: from a sales representative offering modern digital devices to an ordinary consumer using these devices and software in everyday life.
Research has shown that the digital revolution is changing business models, manufacturing and competitiveness. Over the past two years, the vast majority of enterprises have been using information and communication technologies. The analysis showed that digital business models tend to differ depending on the size of business structures and technologies. Businesses use ERP systems when they reach a critical level, allowing them to cope with the complexity and significant time, financial resources, and retraining required to implement ERP. Thus, the gap in the distribution of ERP is much larger between the structures of medium and small businesses than between the structures of large and medium businesses.
Intersectoral differences in digitization are significant. In knowledge-intensive sectors, enterprises are more intensively using all types of technology, and some aspects of digital transformation are almost complete – for example, the average share of employees with access to connected devices is around 90%, compared to 50% in all sectors.
In order to unify the process of studying the conditions in which digital innovations and entrepreneurial activity take place, a methodology is proposed for assessing the country's economy regarding digital transformation. No significant relationship was found between the level of digitalization and the overall performance of the company. This may be due to the fact that the companies under study are not clearly perceived by specialists and information technology leaders due to the lack of digitalization, and in most cases are not subject to strategic planning. Infrastructure companies are more likely to see tangible results in performance assessments such as improved accuracy and quality. The banking sector will benefit by increasing the flexibility of processes, strengthening their focus on customer needs, increasing sales and the emergence of fundamentally new products. The industrial sector indicates a low return on projects in terms of increased sales and the emergence of new customers, as well as the emergence of fundamentally new products, services and opportunities.
A significant relationship between organizational digital culture and the level of digitalization was not identified due to the low level of staff involvement in the digital development project. The digitalization of business processes will give impetus to the total complexity of all professions, on the one hand, freeing up the time of employees to solve more complex and creative tasks. On the other hand, it will significantly increase the requirements for their qualifications. Activities have been developed to support digital security risk management and enterprise resilience.

***Keywords:** digitalization, security, innovation, technologies.*

Introduction

Rapid reductions in computing costs, the emergence of the Internet as a means of communication, the rapid development of mobile Internet, the proliferation of everyday applications and the growing role of social networks and commercial platforms are significantly affecting the functioning of the economy and have a strong impact on business, community organizations and privacy. New digital technologies, such as the Internet of Things,

artificial intelligence and big data, are leading to further disruptive innovations and the creation of new opportunities and challenges.

Digitalization has brought many benefits to consumers and businesses, but it has also created new challenges. Leading scientists of different countries are engaged in research on the development of the digital economy, including Dannikov and Sichkarenko (2018), Kolyadenko (2016), Gudz (2018), Matveychuk (2018), Haanaes & Fjeldstad (2018), Carlsson (2004), Ayres and Williams (2004), and others.

The object of this research is the processes of formation and functioning of the system of economic security of entrepreneurial activity in the conditions of the development of the digital economy.

In the process of writing this study, the author used general and special methods that allowed for the systematic investigation of the problem of digital security of business in the digital economy. In particular, the following methods were used: multidimensional factor analysis; statistical analysis; modeling of structural equations; and strategic analysis.

The main body of the paper

Given its significant impact on the current state of business, production and consumption models, the issue of digitalization needs further study.

There is a need to study how the current digital revolution and information and communication technologies (ICT) affect the economy and what problems are holding back their development in Ukraine.

The *digital economy* is a term that captures the impact of digital technologies on production and consumption patterns. This includes how goods and services are bought, sold and paid for. This term has evolved since the 1990s, when the focus was on the impact of the Internet on the economy. This has been expanded to include the emergence of new types of digital-focused firms and the production of new technologies. Today, the term encompasses a dizzying set of technologies and their applications. These include artificial intelligence, the Internet of Things (IoT), augmented and virtual reality, cloud computing, blockchain, robotics and autonomous vehicles.

It is recognized that the digital economy includes all parts of the economy that take advantage of technological change that leads to the transformation of markets, business models and day-to-day operations. The digital economy covers everything from traditional technologies, media and telecommunications to new digital sectors. These include e-commerce, digital banking and even traditional sectors such as agriculture, mining or manufacturing, which are affected by the use of new technologies. Thus, the digital economy will become a normal economy as the absorption and application of digital technologies in all sectors of the world increases.

Today, Ukraine is actively implementing measures to digitize its economy. Digitalization of the economy is not an end in itself, but only serves as a tool to achieve the strategic goals of Ukraine and the vision of the Ukrainian economy in 2030 (Digital Agenda, 2016; National Economic Strategy of Ukraine 2030, 2021). Digitalization of the economy will contribute to:

- creating conditions for increasing the capitalization of Ukrainian business;
- implementing the technological development of the Ukrainian economy;
- increasing the competitiveness of the Ukrainian economy in global markets.

Table 1. Stages of implementation of digital technologies

Source: Kolyadenko (2016), Digital Agenda (2016), National Economic Strategy of Ukraine 2030 (2021)

Stage	Participants in the process	Example
1. Digital core	Physical technology providers	Semiconductors and processors
	Device suppliers	Computers and smartphones, software and algorithms

	Internet providers	Internet and telecommunication networks
2. Digital providers	Parties that use these technologies to provide digital products and services	Mobile payments, e-commerce platforms or machine learning solutions
3. Digital programs	Organizations that use digital provider products and services to change the way they do business	Virtual banks, digital media and e-government services.

To understand the trends in the digital economy, a study of the stages of implementation of digital technologies in economic activity was conducted (Table 1).

Thus, the chain of digitalization development in the country can be traced: from a sales representative who offers modern digital devices to an average consumer who uses these devices and software in everyday life.

The introduction of digital technologies will help business structures:

- to do business differently, as well as more efficiently and cost-effectively;
- to open many new opportunities;
- to offer goods and services to more consumers, especially those who previously could not be served;
- to experience new market structures which remove, among other things, transaction costs in traditional markets;
- to obtain and analyze large amounts of data.

There is a need to study the current state of Ukraine's economy regarding the introduction and development of digital technologies both at the national level and at the enterprise level. First of all, an analysis of the factors hindering the digital transformation of entrepreneurial activity was conducted. This study was conducted in Ukraine and covered the following topics:

- general information about the company/institution;
- infrastructure and services;
- sales and supplies;
- management practice;
- degree of competition;
- innovations;
- power;
- use of top management's time;
- land and permits;
- crime;
- finance;
- relations between business and government;
- labor;
- business environment;
- efficiency;
- module of green economy;
- aspects related to the environment;
- environmental impact;
- governance and the environment;
- environmental policy and regulation;
- the impact of the institution on the environment.

Enterprises of various forms of ownership and sizes took part in the study. Regional stratification was carried out in the following oblasts: Rivne; Sumy; Zaporizhia; Vinnytsia; Zhytomyr; Dnipro; Kharkiv; Poltava; Kherson, Nikolaev; Odessa; Kyiv.

The number of interviews in the institutions contacted was 8.9%. This number is the result of two factors: explicit refusal to participate in the survey, which is reflected in the rate of deviation (including the deviation of the examiner and the main survey); and the quality of the sample, as represented by the number of unavailable units.

Particular attention was paid to the correct calculation of weights. It was necessary to accurately adjust the results in each region/industry/size to take into account the presence of inappropriate units (if the company ceased operations or was out of reach; for educational or government agencies who answer after calls on different days of the week and at different times; and for cases with no sound in the phone line, where answering machines or faxes were reached, or where an incorrect address was listed and the authors failed to find new links). The information needed for the adjustment was collected at the first stage of implementation: the screening process. The survey was conducted according to a two-stage procedure. A telephone questionnaire was first used to determine eligibility and appointments. Then there was a face-to-face interview with the head/owner/director of each institution.

The results of the study are provided in Table 2. Given the fact that digitalization is global in nature, the analysis was conducted in comparison with other European countries.

Table 2. Analysis of the factors hindering the digital transformation of entrepreneurial activity

Source: Schwab (2019); National Bank of Ukraine (2020)

Safety indicator	Ukraine	The average in Europe	Divergence
Percentage of enterprises that pay for security	78.2	55.5	−22.7
Average security costs (% of annual sales)	2.3	3.5	1.2
Percentage of firms affected by the digital threat	18.8	16.2	−2.6
Average losses due to digital security (% of annual sales)	3.5	5.1	1.6
Percentage of businesses that identify digital security as a major constraint on business	30.9	17.2	−13.7
Labor potential			
Percentage of enterprises offering formal training	24.3	32.2	7.9
Years of experience as a top manager in the enterprise sector	18.1	18.0	−0.1
Proportion of skilled workers (of all production workers) (%) *	89.4	76.6	−12.8
Percentage of enterprises that define labor standards as the main constraint	19.9	10.7	−9.2
Percentage of workers with sufficient digital technology skills	37.9	20.5	−17.4
Factors hindering business development			0.0
Percentage of enterprises that chose access to finance as the biggest obstacle	13.9	14.4	0.5
Percentage of businesses that chose business licensing and permits as the biggest hurdle	0.7	2.6	1.9
Percentage of enterprises that chose corruption as the biggest obstacle	17	7.1	−9.9
Percentage of companies that chose courts as the biggest obstacle	2.2	1	−1.2
Percentage of enterprises that chose crime, theft and disorder as the biggest obstacle	1.6	2.8	1.2
Percentage of enterprises that chose customs and trade as the biggest obstacle	2.2	3.4	1.2
Percentage of enterprises that chose electricity as the biggest obstacle	1.7	9.2	7.5
Percentage of enterprises that chose an inadequately educated workforce as the biggest obstacle	3.9	8.3	4.4
Percentage of enterprises that chose labor standards as the biggest obstacle	2	3	1.0
Percentage of enterprises that chose political instability as the biggest obstacle	25.4	11.9	−13.5
Percentage of enterprises that chose informal sector practices as the biggest obstacle	9.2	12.1	2.9
Percentage of enterprises that chose the tax administration as the biggest obstacle	3.1	4.1	1.0

Percentage of companies that chose tax rates as the biggest obstacle	12.5	13.1	0.6
Percentage of enterprises that chose transport as the biggest obstacle	3.7	3.7	0.0
Capacity of production (%)	68.8	73.2	4.4
Real annual sales growth (%)	−7.7	0.7	8.4
Annual employment growth (%)	0.2	4.5	4.3
Real annual growth of labor productivity (%)	−7.7	−3.3	4.4
Percentage of enterprises that buy fixed assets	37.0	39.0	2.0

Research has shown that the digital revolution is transforming business models, manufacturing and competitiveness. The vast majority of enterprises use at least some ICT. In 2019, an average of 93% of enterprises in European countries had broadband. Virtually all large business structures (98% on average) and more than 91% of small business structures are now connected to broadband. However, the gap between the use of ICT by large and small business structures remains significant.

Business digitization will continue quickly. This will be facilitated by technological developments such as the deployment of 5G networks and increasing the connection of objects via the IoT. However, diffusion remains uneven between business structures. The share of employees who use Internet-connected devices is an indicator of how much ICT has been implemented throughout the business. The proportion of workers using computers with Internet access has grown significantly in Europe over the past decade. However, among small business structures it remains slightly lower compared to large business structures (Figure 1). In 2019, there were significant differences between countries. More than 70% of employees used computers with Internet access in the Nordic countries.

Businesses can choose from a wide range of digital technologies, and websites using broadband Internet are the most common tool (in 2019, 78% of businesses had their own website). Although it is the hallmark of the Internet age, a much smaller proportion of businesses sell through e-commerce. In Europe, only 24% of businesses with at least 10 employees received electronic orders in 2019. This share, which has remained stable since 2016, increased by only 5% compared to 2010. In 2019, e-commerce generated an average of 19% of total turnover. Up to 90% of e-commerce revenue comes from business-to-business transactions through e-commerce programs.

There is a pattern here, in that digitization allows organizations to expand business integration, in addition to managing information flows in companies, for a variety of business functions. Enterprise Resource Planning (ERP) allows business entities to take advantage of higher integration of information and processing into various business functions.

Given the fact that the digital economy primarily affects the development of enterprises whose activities are related to information technology, an analysis of the enterprise for the 2021–2018 period was conducted, the results of which are provided in Table 3.

According to the results, we see growth, but its rate is lower than the rate in developed countries.

Customer Relationship Management (CRM) tools enable business entities to collect, integrate, process and analyze information related to their customers through the intensive use of ICT. Currently, ERP and CRM are used by 36% and 30% of enterprises in Ukraine, respectively, which are 10% higher than they were in 2010 (Il'chenko, 2021). An analysis of the use of ICT tools and activities in European enterprises is provided in Figure 2.

Although most businesses are interconnected, digital technologies are still primarily seen as a means of communication – the level of acceptance tends to decrease as technology improves.

Analysis showed that digital business models tend to differ depending on the size of business structures and technologies. For example, small businesses are less likely to use corporate

resource planning (ERP) systems than large businesses. Businesses use ERP systems when they reach a critical level, which allows them to deal with the complexity and considerable time and financial resources and retraining required to implement ERP.

Thus, the gap in ERP diffusion is much larger between medium and small business structures than between large and medium business structures. The opposite applies to software for supply chain management, cloud computing or big data analysis, for which the digital divide is widening between medium and large businesses.

Digital conversion also occurs at different speeds. For example, small and medium-sized enterprises (SMEs) are catching up with larger enterprises through social media. Conversely, the implementation of software for business intelligence and supply chain management has made little progress in 2014–2020, especially among SMEs. Similarly, the share of SMEs training staff in information and communication technologies has not increased significantly – it remains relatively low.

Table 3. Growth rates of digital technologies in Ukraine

Source: Il'chenko (2021), State Statistics Service of Ukraine (2020)

Field of use	Indicator	Growth rate (changes) of the indicator by years						Average growth rate
		2013 / 2012	2014 / 2013	2015 / 2014	2016 / 2015	2017 / 2016	2018 / 2017	
Information and communication technologies	Enterprises, units	113.1	91.1	104.4	90.7	112.9	109.0	103.1
	Employed workers, persons	99.0	86.8	85.8	93.9	97.6	99.2	93.5
	Value added at production costs, thousand UAH	109.2	120.8	104.4	136.7	115.9	111.5	116.0
Production using high technologies	Enterprises, units	107.8	91.5	96.5	85.8	104.9	104.2	98.1
	Employed workers, persons	97.3	91.4	91.4	96.5	99.8	92.8	94.8
	Value added at production costs, thousand UAH	100.3	104.4	114.6	127.3	108.6	90.2	106.9
Production using mid-level technologies	Enterprises, units	112.7	88.4	102.6	95.0	109.0	105.8	101.9
	Employed workers, persons	95.9	83.5	89.4	96.3	100.7	100.5	94.2
	Value added at production costs, thousand UAH	94.0	101.4	117.1	91.7	125.4	123.1	107.9
Information sector	Enterprises, units	107.1	87.3	97.9	83.0	108.3	104.2	97.5
	Employed workers, persons	99.0	86.7	90.4	97.4	113.0	101.0	97.6
	Value added at production costs, thousand UAH	116.8	113.9	97.4	124.1	162.7	103.9	118.1
High technology services	Enterprises, units	109.3	88.8	101.4	86.0	111.8	107.1	100.2
	Employed workers, persons	97.5	88.1	87.8	94.4	99.6	98.6	94.2
	Value added at production costs, thousand UAH	110.9	105.5	108.0	137.2	116.1	114.8	115.0
Intellectually rich market services	Enterprises, units	109.4	88.8	102.7	90.1	111.3	106.6	101.1
	Employed workers, persons	97.2	89.5	91.9	97.3	97.7	97.8	95.2
	Value added at production costs, thousand UAH	89.1	93.8	108.8	195.8	119.7	105.2	114.4
Services related to the use of computer equipment	Enterprises, units	116.3	92.8	105.8	89.8	117.1	111.8	105.0
	Employed workers, persons	109.7	89.0	94.8	99.3	105.0	105.0	100.2
	Value added at production costs, thousand UAH	143.9	131.2	106.8	170.5	136.4	112.9	132.0

SMEs face several size barriers in terms of the awareness, skills and finances required to implement new digital tools and additional organizational changes. These barriers are a symptom of imperfections in the commodity, credit and labor markets.

The popularity of cloud computing has grown with the explosion of network density and speed and the constant increase in proposed computing power. One third of European businesses buy cloud computing services, an increase of more than 10% in just 5 years. In particular, cloud computing allows small and medium-sized enterprises (SMEs) to access additional processing capacity and storage capacity, as well as databases and software in quantities that meet their needs. In addition to flexibility and scalability, cloud computing reduces the cost of technology upgrades. This frees businesses from previous investments in equipment, as well as from regular maintenance, IT team and certification costs.

More advanced and specialized ICT technologies are less widely used. These include big data analytics (BDA) and radio frequency identification (RFID), where use is limited to certain types of business.

Another major indicator of the development of digital technologies is the prevalence of social media. With its rapidly growing prevalence in society, social media has become a multidimensional vector of information dissemination. Social networking is the most popular activity on the Internet in most countries, used by almost three quarters of Internet users. Companies and other organizations are also increasingly using social media to communicate with individuals (such as potential customers). More than half of the enterprises studied had a presence on social networks. Nevertheless, there is still a marked contrast between countries. Utilization ranges from almost 80% in Iceland and over 66% in Norway, Brazil, the Netherlands, Ireland and Denmark to below 30% in Japan, Poland and Mexico. Medium and large companies are more likely to use social media. Businesses mainly use social media for external interactions. This use includes developing the company's image and marketing products, as well as receiving or responding to customer opinions, reviews or questions. They are much less likely to use social media to engage customers in the development or innovation of goods or services. Social media is also used as a channel for collaboration with business partners, although there are other tools for this kind of interaction. Social media has also become an important tool for hiring employees. Within the European Union, more than half of large business entities used it for recruitment in 2017.

In enterprises, social media is seen as a potential exchange of ideas, opinions or knowledge in the workplace. This use is still relatively low among small businesses (around 12% in Europe). However, this has a significant presence in large business structures (around 30%). For large business structures, the acquisition of social networks is also closely linked to the acquisition of BDA. This illustrates how some businesses are experiencing an integrated digital transformation based on synergies between additional digital technologies.

Regarding the implementation of big data analytics, the study showed that BDA refers to the use of methods, technologies and software to analyze the vast amount of data generated by electronic activity and machine-machine communication (e.g., data obtained from social media activities, production processes). Reducing the cost of storing and processing data has contributed to the collection of large amounts of data and the adoption of BDA. Meanwhile, the expansion of cloud computing combined with the advent of easier-to-use analytical tools has made BDA more accessible to SMEs.

However, large business structures remain the largest and fastest-growing category of users today.

Over the past five years, an average of 12% of businesses in the countries for which data are available have used BDA. This share reached 22% in the Netherlands and over 20% in Belgium and Ireland. In addition, in Belgium and the Netherlands, more than half of large businesses

used BDA. Growth was significant among large business structures and to a lesser extent among SMEs.

The most intensive users of data from the geolocation of portable devices are usually in the field of transport and storage, and to a lesser extent in the construction industry. Businesses in areas such as electricity, gas, air conditioning, water supply and manufacturing are the most intensive users of data from smart devices or sensors. Social media data is mainly used in the accommodation and food and beverage industries. The real estate industry uses social media data to a lesser extent. Data from other sources are mostly used in three areas: information and communication; professional, scientific and technical activities; and real estate activities.

Analysis shows that digitalization has almost no effect on Ukrainian industry, which is showing a tendency to rapidly reduce its pace of development. For Ukraine, the critical problem is the technological backwardness and the preservation of this backwardness. In this regard, Ukraine not only failed to make a technological breakthrough, but also lost its position.

All of this indicates that Ukraine is not ready for the introduction of Industry 4.0 technologies. Moreover, the process of implementing Industry 3.0 has not yet been completed in Ukraine. Even the level of automation in Ukrainian industry is still below average. For example, in metallurgy it is around 50%. Accordingly, the problem of the digital leap, when businesses urgently need to pass level 3.0 and move to 4.0, is very acute in the country.

Cross-sectoral differences in digitization are significant. In knowledge-intensive sectors, businesses use all types of technology more intensively, and some aspects of digital transformation are almost complete. For example, the average share of employees with access to connected devices is around 90% compared to 50% in all sectors. The rate of diffusion in other sectors is much lower.

The introduction and use of ICT in business can be supported in a variety of ways. In developed countries, policies to promote the use of digital technologies by businesses are being intensively implemented. Most often, policy is aimed at business structures, whose goals are to increase profitability. This includes increasing sales, increasing competitiveness, reducing operating costs, reducing compliance costs, and increasing productivity. Policy objectives are also formulated at a more macro level in terms of stimulating growth and employment.

Using digital tools and technologies is an effective means to achieve these goals. Thus, in order to achieve the goal specified in the national program of digitalization of the economy, it is necessary to develop a program for the development of entrepreneurial activity in the context of digitalization. The main measures should be aimed at providing businesses with access to the knowledge and skills needed to choose and use the tools that will benefit them most. Second, they must help businesses implement digital tools, which may include the need to finance investment costs.

It is also necessary to use information campaigns on issues such as digital security and confidentiality, which many countries identify as key areas of economic security of business in the context of the digitalization of the economy. Technology-specific policies tend to be more narrowly targeted at specific companies or sectors, as well as network operators and relevant researchers.

A number of countries support the development and implementation of innovative products, especially digital services, to increase competitiveness and thus stimulate growth. The development and implementation of specific border technologies is a popular policy area. Artificial intelligence is most often mentioned, as well as 5G, IoT, blockchain, robotics, quantum technology and others. Data generation, collection and analysis are also highlighted as important supporting factors. At the same time, several countries emphasize the need to promote efficient technology and data markets.

Reducing digital disparities is also a stated policy goal in some cases and can often be linked to high-level welfare goals. Meanwhile, a number of countries have highlighted policies to

strengthen government implementation of digital technologies to increase efficiency, including the modernization and automation of tax systems. Several countries have targeted action in the social sectors where the government is usually active, such as promoting e-health.

Given the ongoing debate and the lack of consensus among digital development theorists and practitioners on ways and methodologies to measure the scale of the digital economy and the impact of digital transformation, an analysis of the state economy's capacity for digital transformation was conducted.

Thus, the results of the analysis prove that there should be: the implementation of developed strategies and efforts to accelerate the pace of transformation of the private and public sectors; the raising of public awareness of the use of digital technologies, strengthening the interaction of the scientific and educational community with the private and public sectors; and the creation of a business environment conducive to innovation, R&D and entrepreneurship. All of the above are key elements of the digital economy culture and tax environment, and stimulating investment in innovation and entrepreneurship development should be a priority of public policy.

It is recommended to use a number of policy tools to promote the use of ICT in business. The most widely used measures are direct financial support, followed by non-financial support. Indirect financial support, along with regulation and legislative guidance, is less often a tool of choice (Table 4).

Direct financial support includes grants to help target companies cover the cost of access to digital technologies and tools. For example, South Korea has offered grants for cloud services. For its part, Portugal offered direct financial support for the development and maintenance of websites, e-commerce, Internet marketing and big data.

In countries such as Denmark, Slovenia and Germany, direct financial support can also help businesses develop digitization strategies or increase digital capabilities and skills. Although they do not directly promote the use of digital technologies by businesses, many countries note the availability of grants or vouchers to support research and development (R&D) and other innovation activities. This support can contribute to technological progress and the development of innovative products for commercialization.

Indirect financial support includes tax credits or other benefits for ICT investments (as observed, for example, in Brazil and Japan). It also includes broader tax support schemes for research and development, including for digital technologies. Many European countries have such general support for research and development, including some who have stated that they do not have policies to promote the use of digital technologies in business. Competence centers offer measures to increase knowledge and awareness of digital technologies and related opportunities and risks.

For example, Australia, Lithuania, Sweden and Singapore provide special business advice and consulting services. Turkey provides special advice on regulations on new business models, with responses agreed between governments, while Latvia and Norway offer training. Countries such as Portugal and Slovenia give companies the opportunity to share experiences by demonstrating digital champions, group seminars, mentoring schemes and similar initiatives.

Digitization makes it easy to store and change information and knowledge. Digital technologies are creating a system of mass media and communication that increasingly connects all parts of social and economic life. In order to unify the process of studying the conditions in which digital innovations and entrepreneurial activity take place, a method of assessing the country's economy to digital transformation is proposed (Figure 1).

Table 4. Policy tools to facilitate the digital takeover of businesses by type of tool
Source: Schwab (2019); State Statistics Service of Ukraine (2020)

Countries	Financial support		Non-financial support	Regulations and legislative instructions	Together
	Direct	Indirect			
Australia	2	2	2	1	7
Austria	1	1	1	1	4
Chile	..	..	1	1	2
Colombia	1	1	1	1	4
Czech Republic	..	..	1	2	3
Denmark	2	..	3	2	7
Estonia	2	..	2	..	4
Finland	1	..	..	..	1
Germany	2	..	3	3	8
Israel	1	1	..	..	2
Japan	1	2	..	..	3
Korea	3	..	..	..	3
Latvia	2	1	1	3	7
Lithuania	1	1	1	1	4
Netherlands	..	1	..	..	1
Norway	1	..	1	1	3
Portugal	1	1	1	..	3
Slovenia	1	..	1	..	2
Spain	1	..	..	..	1
Sweden	2	0	2	1	5
Turkey	1	..	..	..	1
Brazil	..	2	..	..	2
Costa Rica	..	..	1	..	1
Ukraine	3	1	1	1	6
Singapore	..	..	1	1	2
In total	**29**	**14**	**24**	**20**	**87**

This methodology is based on econometric analysis to assess the impact of cultural, geographical, regulatory and commercial barriers on digital transformation.

Normative acts and legislative instructions are used to create legal bases in a wide range of areas. Coordination of efforts to strengthen cybersecurity is needed, including regulatory changes to codify the role of the National Agency for Cyber and Information Security. One such principle is to promote the integration of new business models in a technology-neutral way to ensure user-friendly digitization.

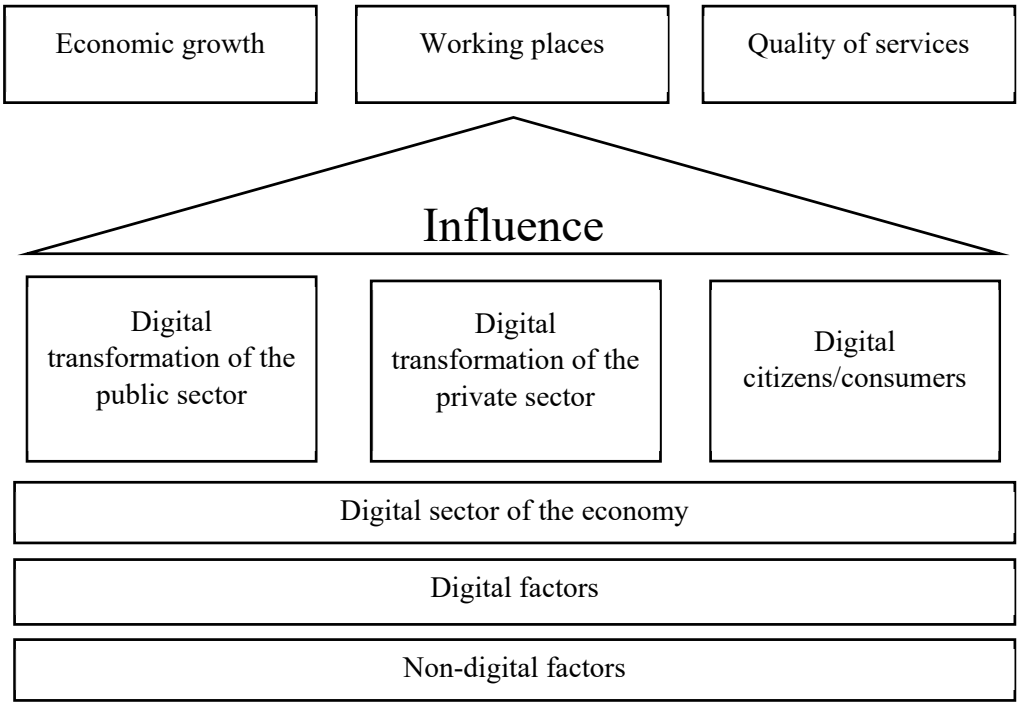

Figure 1. Methods for assessing the country's transformation towards a digital economy
Source: developed by the authors

Methodology for assessing the digital security of business

Digital security incidents harm businesses, governments and individuals by undermining the availability, integrity and confidentiality of their data, information systems and networks. Entrepreneurial structures suffer material and intangible losses, including monetary losses, loss of competitiveness, damage to reputation, interruption of operations and breach of confidentiality. With the advent of the consumer and industrial Internet of Things, which connects to the Internet, the damage can spread to the physical environment and affect security. There is a need to study trends in digital security risks and digital security policies. The focus is on policies that encourage digital security innovation, improve digital product security, and improve vulnerability management. This also opens up new opportunities for artificial intelligence regarding digital security.

The risk of digital security arises from incidents caused by threats to vulnerable sites. Sources of threats include governments, groups, and individuals with malicious or criminal intent. Their motivation varies, but usually includes the geopolitical goals of governments. Incidents can also be caused by unintentional threats, such as human error or power outages.

Analysis of the types of security related to digital technologies in the world reveals the most common:

1. Distributed Denial of Service (DDoS) attacks are a common type of incident that disrupts an Internet service by flooding it with illegitimate requests. Data on DDoS attacks usually come from companies that offer DDoS mitigation services. They do not have a comprehensive picture of the landscape, but can provide useful information on key trends. For example, according to Netscout, the scale of the largest DDoS attacks has increased over time. In 2005, the largest attacks reached 11 Gbps, 50 Gbps in 2009, 100 Gbps in 2010, 500 Gbps in 2015, and 800 Gbps in 2016. In 2018, one reached 1.7 Tbit/s (Netscout, 2019).

In 2018, the frequency of large-scale DDoS attacks decreased year-on-year, while attackers increased the size of smaller attacks in the range from 100 Gbps to 200 Gbps. This is still high for most online services. DDoS attacks do not need to use such high bandwidth to block online

services. In 2018, 96% of DDoS attacks consumed less than 10 Gbps. Meanwhile, 91% of businesses that suffered DDoS attacks said that at least one attack completely saturated their Internet bandwidth (Netscout, 2019). Although the longest attack in the third quarter of 2019 lasted more than 20 hours, 85% of attacks lasted less than 90 minutes; only 0.78% lasted more than 20 hours (NexusGuard, 2019).

2. Phishing remains common and is more difficult for humans to avoid. In phishing, one of the main vectors involves attackers disguising themselves as a reliable person in Internet communication. In this way, they receive confidential information, such as usernames and passwords, or deliver malicious code. There are different types of phishing attacks. Phishing reports often contain links to malicious websites that are becoming increasingly difficult for end users to detect without the use of automated protection. Extensive non-targeted campaigns aim to collect data by directing users to fake e-commerce or financial websites. More sophisticated emails are aimed at specific people so that they embed malicious software in their organization's information system (speech phishing).

In the countries of the European Union, phishing and farming (which redirect to fake websites that acquire personal information) differ greatly from country to country. Various factors may help explain these differences. These include lack of awareness/understanding of phishing attempts and/or inability to identify them, national languages, security measures offered by e-mail and Internet Service Providers (ISPs), etc. According to Symantec (2019), underwater phishing remained the most popular target of targeted attacks in 2018. This was used by 65% of all known cybercrime and government groups. According to Verizon, 32% of data breaches in 2018 were related to phishing activities. Phishing was present in 78% of cases of digital security espionage, including the installation and use of backdoors (Abid & Jemili, 2020).

3. Measuring software is a type of malicious software that uses cryptography to restrict or disable data availability and requires ransom to recover. Extortion programs are a form of digital extortion (Ebers & Steinrötter, 2021). Despite the fact that the required programs have existed for many years, this came into broader public focus in 2017.

These high-profile attacks have helped raise awareness of digital security and encouraged many businesses and organizations to step up their core security measures, including backup and recovery plans.

The extortionist can paralyze physical operations in factories and production environments. If an attacker gains access to an information technology (IT) system, they can successfully target an operational technology (OT) infrastructure that manages physical installations.

4. Cryptocurrencies have, over the past five years, been the target of various tools seeking to take advantage of the growing interest in them. Most cryptocurrencies are stolen from cryptocurrency exchanges. In the period from 2012 to 2019, at least 42 successful attacks were listed on the stock exchange. For example, in 2019, 12 attacks led to the theft of cryptocurrencies worth $292 million. In 2018, eight attacks led to the theft of $844 million. Some of these attacks have led the affected companies to bankruptcy (e.g., Mt. Gox, Cryptopia, Youbit). In some cases, partial amounts were collected or reimbursed to customers. Other attackers take control of a blockchain that supports cryptocurrency. In 2018, Bitcoin Gold (BTG) was excluded from the Bittrex cryptocurrency exchange after an initial attack of 51%. The attackers took over most of the network's computing power to reorganize the blockchain, which involved a cost of $18 million (Canellis, 2018). In January 2020, another 51% attack doubled BTG by $72,000. In 2018, Ethereum Classic suffered a similar attack of 51% of the total amount of Ethereum Classic (ETC) coins, for $1.1 million (Beedham, 2019).

Over the last three years, more inconspicuous techniques such as cryptocurrency and cryptojacking have been developed. Cryptojacking occurs when criminals install malicious software that usurps a user's processing power to extract cryptocurrency. Cryptojacking is cryptocurrency using scripts embedded in web content running in a user's browser.

5. Malicious software is becoming more sophisticated. File-free malware is less visible because the code runs only in system memory or uses commonly allowed tools installed on the system. Malicious software has evolved from encrypted to oligomorphic to polymorphic and metamorphic. Encrypted malware is the first step to avoid signature-based detection. With each infection, the malware is encrypted with a different key, making each file unique. However, security features can still detect a decoder that is part of the code that decrypts it and remains the same among infections.

Oligomorphic malware can change its decryptor with each generation of malicious code – that is, each time the code is distributed elsewhere. However, this technique can only create a few hundred different generations, which is not enough to avoid security.

Polymorphic malware can create countless decoders through the mutation mechanism, and cannot be detected by simple signatures.

Metamorphic malware can completely rewrite your code. Thus, each new version distributed elsewhere no longer corresponds to the previous iteration without the use of encryption.

Thus, there is a need to develop measures to manage digital risks in business.

Given the complexity of digital security risk management, it is difficult to quantify the extent to which companies implement best practices in this area. However, certain statistics provide useful information. They measure specific aspects that can be used as proxies to form a relatively strong picture of Ukraine's situation. They concern business entities that assess digital security risks, inform their employees about digital security commitments, conduct security tests or regular backups, and insure against digital security incidents.

Digital security risk assessment – a periodic assessment of the likelihood and consequences of digital security incidents – is the basis for digital security risk management. In general, the share of enterprises conducting risk assessment ranges from 14% in Ukraine to 60% in Finland. As for other indicators of digital security, this share increases on average with the size of firms. This is less than one third among small firms, but almost three quarters among large firms.

Digital safety risk assessment is extremely important to help decide what to do with risk. Risk can be reduced or transferred – it can also be accepted or eliminated, although elimination eliminates both risk and benefit. To reduce risk to an acceptable level, firms must choose security measures that are proportionate to the risk and context. Too much security hinders economic and social activities protected by security measures. Too little security will not reduce risk enough. Security measures may include security tests, backup procedures, cryptographic techniques, two-factor authentication, network access control, and the use of VPNs.

The analysis showed that the practice of risk assessment significantly correlates with security tests or backup procedures.

As observed for other ICT security indicators in this section, large businesses are on average much more likely to implement security than small ones. In addition, the variability in different countries is relatively similar between large and small structures for safety testing. This suggests that backup in large enterprises is part of core digital security practices, while in SMEs it is more sensitive to risk assessment practices.

One way to reduce risk is to decide on the transfer of risk by purchasing insurance. The propensity of businesses to purchase insurance policies varies widely, from 4% in Lithuania to over 56% in Denmark. In all but two EU countries, the propensity increases with the size of enterprises. In Denmark, it is significantly higher among small enterprises (57%) compared to medium (5%) and large (40%). This is also the case in Slovenia, although to a much lesser extent (Figure 1). In general, the propensity to buy insurance can be seen as an indication of how seriously firms take digital security. However, it also depends on the availability of insurance policies in the country that cover the risk of digital security. The digital security

insurance market is complex, and includes traditional insurance policies or stand-alone policies.

Another indicator of commitment to digital security is the share of enterprises that inform working people about their commitments on ICT security issues. This ranges from one third in Greece to more than three quarters in Ireland, where there is also a high concentration of business in the ICT sector, often a multinational bridgehead for Europe. This share also increases with the size of enterprises: less than 60% among small enterprises, but more than 90% among large enterprises.

More generally, all of the above indicators, based on Eurostat data, clearly show that firms' propensity to implement digital security measures increases with their size. In addition, this propensity is also systematically higher for firms in certain fields, such as the ICT sector, or professional, scientific and technical activities. In addition, the risk assessment is also higher, on average, in real estate.

It has been proven that there are obstacles to the widespread adoption of a digital security system. Many politicians are still unaware of the need to remove such barriers and encourage responsible behavior by all stakeholders.

This analysis allows recommendations for digital security to be developed. They aim to focus on what is critical to the economy and society, without imposing unnecessary burdens on others. The main areas are:

- adaptation of their comprehensive policy;
- ensuring that operators effectively reduce the risk of digital security to critical functions to a level acceptable to society;
- promoting and building partnerships based on trust;
- improving cooperation at the international level.

These recommendations also clarify how this area relates to broader national risk management policies.

This process should be based on a national risk assessment covering all economic and social activities.

The Government, working with relevant public and private entities, determines:

1. Critical activities related to digital security.
2. Operators of these important activities at enterprises.
3. That cyclical risk management is carried out to identify functions without which they would not be able to perform effectively.
4. That a map of the digital ecosystem, i.e., the digital environment that supports their functions along the value chain, is compiled.
5. The digital security risks of critical functions are cyclically assessed, taking into account their digital ecosystem, and the level of digital security risk to be reduced, transferred, avoided and accepted is determined on this basis. This involves risks and digital security management measures, as well as those that protect activities, detect and respond to incidents and establish resilience.

The first three stages of this process are part of a broader national risk management system and critical infrastructure protection policy, and focus on digital security. It is important to mention them in order to ensure the coordination of stages four and five with the national risk assessment and not to create an unnecessary burden for operators.

Considering the activities in accordance with the provided recommendations, this will create additional restrictions for operators and may affect their competitiveness in the global market. Therefore, governments often work with these operators and other stakeholders in the first and second stages, and more generally in the policy-making process, to best balance progress in digital security with economic and social indicators.

Step four introduces the concept of the digital ecosystem, which is broader than information systems and networks and includes digital assets such as hardware, software, networks and data, operational technologies that detect or cause changes in physical processes, and internal and external entities, individuals and processes that design, maintain and operate them, and the relationships between them. Step four is a prerequisite for step five, where operators manage digital security risk, i.e., as part of their broader enterprise risk management system and overall economic and social decision-making processes.

Given the role of digitization in stimulating the development of new sources of sustainable growth, innovation, employment, prosperity and inclusiveness, in order to maximize the economic and social benefits of the digital economy, enhanced mechanisms are needed to involve all stakeholders in policy development processes, including governments, international organizations, business, civil society, organized labor, the technical Internet community and academia.

It has been proven that the strength and dynamism of the digital economy depend on the efficient access of users and innovators to communication infrastructure and services through high-speed networks, more efficient use of digital technologies by businesses, governments, individuals and society, openness and trust.

This is further recognition that policy-making related to digital transformation requires an integrated public approach and cooperation with all relevant stakeholders.

Digital dependence on critical activities has increased and is now accelerating through the digital transformation and generalization of technologies such as big data, artificial intelligence and the Internet of Things. At the same time, digital security threats are growing in number and quality. Many governments expect that in the coming years, digital security incidents affecting critical action could lead to major catastrophes.

According to the results of the study, measures are proposed to address the issues of digital security of business. Their implementation provides a solid basis for strengthening the digital security of economic and social activities without reducing the opportunities provided by digital transformation.

The introduction of these measures in practice will help strengthen the digital security of individual enterprises without imposing unnecessary burdens on other entities.

As already proven:

– Digital transformation affects all economic and social activities, stimulating innovation and bringing significant benefits, but also exposes these activities to the growing risk of digital security;

– Digital security risks arise from intentional or unintentional threats that are transboundary, exploit vulnerabilities, and cause incidents that affect the availability, integrity, and confidentiality of the data, hardware, software, and networks on which they operate;

– The multiplicity and complexity of digital relationships between sectors, as well as along value chains, creates a common digital security risk that no one participant in the production process can significantly reduce for all;

– Partnerships in and between the public and private sectors are essential for a coherent and holistic approach to digital security risk;

– Measures taken by different operators in different sectors and countries depend on the same digital technologies and can therefore be simultaneously affected by threats that share a common vulnerability;

– Digital security incidents can spread extremely rapidly between operators, sectors and borders;

– Disruptions to critical actions caused by digital security incidents in one place may spread to other operators, sectors and countries, potentially affecting regions and international stability;

– The consequences of digital security incidents may go beyond the interests of these operators, affect society as a whole and others abroad, and as a consequence any residual risk taken by these operators could affect all those dependent on such activities, as well as society as a whole;
– Improving the digital security of activities is a priority of national policy;
– Differences in public policy in different countries increase the complexity of managing digital security of interdependent critical activities abroad, and international cooperation is crucial to reducing such differences and maximizing the global effectiveness of domestic policies;
– Digital security risk management must respect the confidentiality and protection of personal data.

Thus, the digital ecosystem means a digital environment that supports enterprises in the value chain of critical activities. It includes digital assets such as hardware, software, networks and data, operational technologies that detect or cause changes in physical processes, and internal and external entities, individuals and processes that design, maintain and operate them, and interact with them.

Developing a strategic approach to digital security risk management should be done by:

1. Adopting at the highest level a national digital security strategy, which sets clear goals for strengthening digital security and resilience to activities, as well as ensuring coherence with national risk assessment and other risk and sector strategies.
2. Establishing an internal governance mechanism that distributes authority and responsibility among specific structures for the development and implementation, together with relevant stakeholders, of policies to enhance digital security within and between sectors.
3. Ensuring internal coordination in order to:
- establish cooperation, taking into account the importance of dialogue between digital security and industry experts;
- ensure the consistency of measures;
- provide the efficient allocation of resources.

Businesses are encouraged to increase their capacity to support digital security risk management and resilience by:

1. Developing new or enhanced incident response capabilities, for example through one or more computer emergency response teams (CERTs), computer security emergency response teams (CSIRTs) and/or security centers (SOCs) responsible for monitoring, preventing, and recovering, as well as mechanisms to promote closer cooperation and communication among those involved in responding to incidents.
2. Promoting cooperation between CERT/CSIRT/SOC and operators, including incident reporting and analysis, to facilitate rapid and effective operational cooperation.
3. Application of best practices in digital security risk management related to the provision of important digital measures by the government.
4. Promotion of international digital security standards, methodologies, basic security manuals, best practices and tools.
5. Providing support to operators by exchanging information on threats, vulnerabilities and risk management practices.
6. Promoting the development of a global market for a variety of reliable security services and products, including managed services, audit and response services, including, where appropriate, a range of mechanisms for reliable signaling of the nature and level of security.
7. Supporting the development of a skilled workforce that can manage cross-sectoral and sectoral digital security risks.

8. Adopting and encouraging the adoption of responsible and coordinated processes for the detection and management of vulnerabilities, as well as the encouragement and protection of security researchers.
9. Sharing, in accordance with operators and other entities, properly compiled statistics on incident reporting.
To effectively reduce the risk of digital security to a level acceptable to society, consistent with the national risk assessment, a mechanism for reducing the risk of digital security, which includes measures to manage, protect, detect and respond, was created (Figure 2).

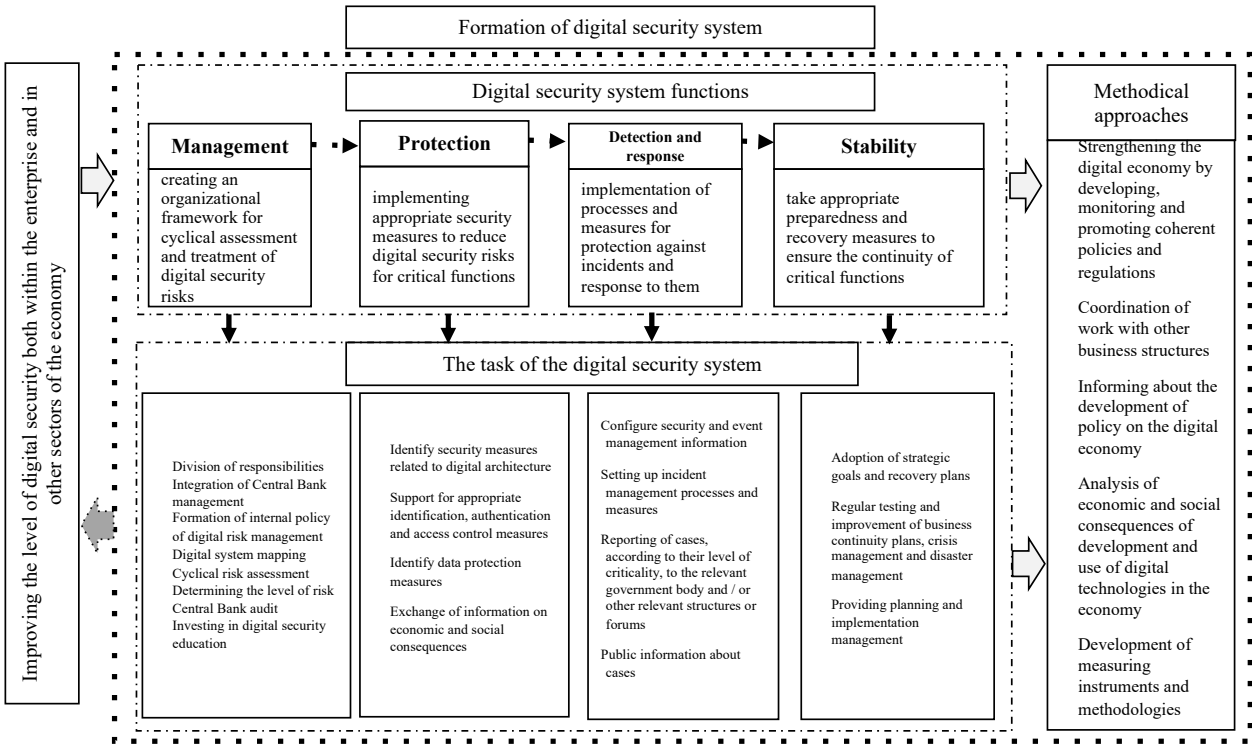

Figure 2. Digital security mechanism
Source: developed by the authors

During the implementation of the mechanism of digital security, the following methods of work are offered:
1) Strengthening the fundamentals of the digital economy by developing, monitoring and promoting a coherent policy and regulatory framework, including:
a) stimulating competition and investment in high-speed broadband and promoting convergence and universal access to broadband networks, services, programs and devices;
b) promoting investment in digital technologies and knowledge-based capital and improving the availability and use of data;
c) reducing barriers to access and use of digital technologies;
d) promoting research, innovation and new business opportunities, including those arising from new technologies and applications, while considering their economic and social implications and assessing the appropriateness of policy and regulatory frameworks and global standards;
e) strengthening confidence in the digital economy, including through the promotion of digital security risk management for economic and social activities and the protection of confidentiality, as well as the development of data transfer strategies and international arrangements that promote interoperability between systems.
2) Coordinating work with other business structures in order to:

a) develop analyses, policies and best practices that use the potential of digital transformation for growth and prosperity by strengthening entrepreneurship, ICT skills and employment and improving health, well-being and aging;
b) further develop and implement medium and long-term roadmaps for digital transformation.
3) Informing on the development of policies on the digital economy, in particular by:
a) reviewing and analyzing new technologies;
b) analyzing the economic and social consequences of the development and use of digital technologies in the economy and the impact of digital security and privacy on the economy and society;
c) developing measurement tools and methodologies, including the use of the Internet as a source of statistics, to strengthen the database for the digital economy and assess its contribution to the economy as a whole;
d) participating at the national level in cooperation with other relevant commissions in order to use innovative experience and best practices in individual countries, to provide volunteer countries with an assessment of the degree of digital maturity. This would help policymakers ensure a coordinated and cohesive approach by the government to better respond to digital transformation and make it work for growth and prosperity.
To build trust in sustainable partnerships, it is necessary to develop partnerships for policy development and implementation by:
1. Having open dialogue at the national level between operators and relevant public authorities to identify and implement measures to be taken by operators, taking into account the specifics of each sector, as well as the constraints on business, resources, regulation and the operator market, including small and medium-sized enterprises.
2. Supporting public-private cooperation and structured dialogue between operators within and between sectors, as well as with other relevant private actors (e.g., suppliers) to facilitate the exchange of digital security experiences, threat management and risk management.
3. Continuing ongoing dialogue on digital security with industry experts to improve mutual understanding of their specifics and limitations.
4. Ensuring bilateral and multilateral cooperation in order to exchange knowledge and experience on internal policies, practices and models of coordination with operators and to promote collective action.
5. Supporting cross-border cooperation and exchange of information on public-private research and development on digital security of critical activities, including methodologies for assessing the impact of digital security incidents.
6. Supporting cutting-edge research, fostering innovation, and working together to develop digital security risk management skills and knowledge that will help build a skilled workforce for the future.
Most economic and social activities are digital. Among these activities, some are critical, as their interruptions or disruptions can have a serious impact on: the health, safety and security of citizens; the effective functioning of services important to the economy and society; or economic and social prosperity in a broader sense.
The implementation of the proposed mechanism will help raise awareness of the need to develop policies to better protect information systems and networks that support business. However, such policies should not undermine the benefits of digital transformation in critical sectors through constraints that hinder innovation or unnecessarily restrict the use, dynamism and openness of digital technologies.
The modernized digital security framework will serve as a forum for (a) exchanging information on digital security activities to identify best practices in coordination with other international fora and (b) developing analytical work to support implementation.

Assessment of the impact of the human capital management system on digitalization and the overall level of economic security. Today, the use of digital technologies is perceived by the management of many Ukrainian enterprises as a purely technological task. However, the meaning of digitization is such that it is not so much technology that changes, but the system of human capital management and organization of the enterprise. Improving the level of digitization is the task not only of specially appointed IT professionals, but also of all employees of the company, from the CEO to regular contractors and employees. Without an understanding of the systemic changes taking place in the digital economy, it will be very difficult for domestic enterprises to withstand competition in current and future markets.

There is a need to study how the implementation of a human capital management strategy affects digitalization and the overall level of economic security of a business. Empirical analysis is performed by the method of structural equations. It is obvious that structural and social components need to be integrated when planning an effective human capital management strategy in the context of business process digitalization, but the issue of empirical evaluation is still relevant. Digital technologies have a significant contribution to the overall economic security of enterprises in the digital economy.

Digitization is a factor in the competitiveness of enterprises which reduces costs by up to 25%. Therefore, in international competition, companies need to actively implement digital technologies and, as a result, new approaches to human capital management from the standpoint of the development of organizational digital culture and digital knowledge. Thus, the first hypothesis for further empirical analysis is that the level of digitalization of the enterprise has a significant relationship with the overall organizational digital culture, which is expressed in increased sales, reduced resource intensity and complexity, and the emergence of new consumers, new products, services and opportunities, and thus is one of the fundamental factors of economic security.

Organizational digital culture includes values such as novelty and digital innovation, as well as digital technologies aimed at improving economic efficiency. Each of its elements has a strategic basis, while the very concept of organizational culture is the subject of a separate study. This study is important for its predictions on the human capital management strategy. Kharchyshyna (2008), Grishnova (2014), Bogashko and others studied the elements of organizational culture in human capital management, highlighting such elements as learning, motivation and internal communication. In order to formulate a special element of the general organizational culture related to the principles of human capital management, we use the term *digital culture*, which understands the intrinsic values and expectations shared by employees and aims to develop and implement digitization to systematically achieve the overall performance of the enterprise. In general, digital culture is shaped by the internal goals of human capital management and is based on the principles of governance at all levels. The specifics of business processes and organizational culture in enterprises with a low level of digitalization is manifested in outdated processes and regulations, overly strict requirements for infrastructure, and the use of outdated management methods and information transmission systems. The task of senior management is to transform organizational culture to provide increased flexibility, transparency of goals and digitization, and measures aimed at the development and practical implementation of digitization to systematically achieve the overall performance of the enterprise.

Digital organizational culture includes:

1. Interaction with the help of digital technologies by interacting with a variety of digital technologies and identifying appropriate means of digital communication in context.
2. Exchange through digital technologies, involving sharing data, information and digital content with others using relevant digital technologies that act as intermediaries in the exchange.

3. Public participation through digital technologies, where the organization can participate in society through the use of public and private digital services.
4. Cooperation with the use of digital technologies, via the use of digital tools and technologies to work together and share resources and knowledge.
5. Internet etiquette, which involves knowledge of the rules and norms of behavior in the process of using digital technologies and communication in digital environments, the adaptation of communication strategy to a specific audience, and understanding and taking into account cultural diversity in the digital environment.
6. Digital identity management, which concerns the ability to protect the organization's reputation.

Therefore, the following hypotheses were formulated for testing:
- There is a significant correlation between digital culture and production efficiency.
- There is a significant correlation between digital culture and overall organizational performance. The practice of human resources management includes the full range of applied technologies of planning, organization, control and motivation of employees for the effective operation of the enterprise, implemented on a systemic basis.

Problems of mastering the digitalization of the enterprise note the lack of staff readiness: their technological incompetence and lack of participation and interest.

It has been proven that in the early stages of digital development, most of these problems are less common. This is due to the fact that companies that are at the initial stage of their digital development and are implementing projects at this stage, which can be relatively simple. The main problems of newcomers are related to their lack of experience in project implementation (57%) and lack of qualified managers (49%). Empirical work involves varying degrees of influence of human capital management practices on the level of digitalization of the industry. Foreign scientists such as J. Storey and Kianto et al. (2017), in the example of medium and small business, do not find a significant relationship between the strategy of human resource management and digital strategy, nor the level of digitization. However, these authors emphasize the creation of a new business team culture of thinking and a new organizational culture. Thus, the following hypotheses were formulated:
- There is a significant correlation between the practice of human capital management and the level of digitization of production.
- There is a significant correlation between digital human capital management practices and overall organizational performance.

Digital human capital management tools that integrate social components such as the concept of digital culture and human capital management practices, as well as structural components, are presented as organizational and managerial approaches to new digital knowledge management and known boundaries and have some contribution to enterprise efficiency.

Some scientists (Grishnova, 2014; Petrov, 2019) note that strategic approaches to integrated human resource management are needed to address knowledge and competence issues related to new digital technologies and industrial processes in manufacturing companies, but research is conducted only in the context of a strategic approach to staff development. It is argued that leadership, training and exceptional ability are key factors in stimulating the digital involvement of staff. According to the authors, companies that intensively support the training of employees and students as future professionals practice a consistent policy in the field of digital research. Analyzing the gap between digitization needs and existing technologies, it is possible to identify key areas for digital literacy. As noted in previous sections, the effectiveness of digital technologies is determined by the knowledge and skills necessary for the safe and efficient use of digital technologies and Internet resources. Digital literacy is based on digital competence – the ability to solve a variety of tasks using information and communication technologies (ICT) and to use and create content using digital technologies,

including the search and exchange of information, answering questions, interacting with other people and computer programming.

There will also be a shift in emphasis towards the development of complex, integrated skills for collaboration and communication in the digital environment as opposed to narrowly understood computer literacy. It is important to consider digital skills which cover ICT technical knowledge in close connection with soft skills and general knowledge.

For example, this approach is illustrated in the "Target Competence Model 2025", prepared by the BCG based on the consensus of experts and an analysis of approaches. In addition to the formation of purely technical skills in working with digital devices, this model includes cognitive and socio-behavioral competencies aimed at ensuring a comfortable existence, effective communication and human development in the digital environment. Based on these competencies, we can identify the main areas of development: 1) digital skills and knowledge – for example, basic digital literacy, data analytics, machine learning, artificial intelligence, programming, IT systems architecture, cybersecurity; 2) skills and knowledge that help to cope with instability and uncertainty around the future – for example, adaptability, critical and systematic thinking, the ability to cope with stress, change management, business planning, the ability to self-study in accordance with the concept of lifelong learning; 3) skills and knowledge that help to cope with the large flow of information, including basic skills in programming, retrieval, processing and analysis of information, information hygiene, media literacy, and attention management; 4) skills and knowledge that determine high communication skills for effective interpersonal interaction – for example, the ability to work in a team, cooperation, self-presentation skills, business negotiation skills; and 5) skills and knowledge that the machine cannot master – for example, empathy and emotional intelligence, creativity and non-standard thinking, control of robotic processes.

The work of domestic scientists indicates the need for mass retraining of the laid-off labor force (Yarova, 2015; Fedotova, 2017). This primarily concerns developing digital skills that allow employees to adapt to changing work processes and the requirements of employers. On the basis of the conducted research, we formulate the following hypothesis:

- There is a significant correlation between digital knowledge and the level of digitalization of business processes.

According to the results of the analysis conducted above, it is proved that Industry 4.0 technologies are among the priority factors for competitiveness.

In order to assess the understanding of the impact of Industry 4.0 technologies among staff and to find the factors hindering the introduction of digital technologies in Ukrainian enterprises, a study was conducted.

Respondents showed a fairly high level of awareness of Industry 4.0 and were aware of the factors of competitiveness, almost as much as elsewhere in the world.

The only exception was the factor of "rapid entry into the market of new products." Very few respondents recognized it as an important factor in competitiveness.

At the same time, almost half of the respondents stated that the main barrier in the implementation of modern ICT systems is that they are not the main priority.

This confirms the weak integration of approaches. Against the background of insufficient investment in development, this means that these gaps will widen.

The awareness of all employees of the need for development contributes to the introduction of an effective system of economic security at the enterprise. A study was conducted to assess the effectiveness of the introduction of entrepreneurial culture in enterprises.

Recognizing the importance of development and investment in R&D and human resources, this ultimately concerns short-term survival priorities, profiting by key stakeholders, and ongoing projects. Accordingly, a culture of cooperation based on trust and medium-term development and innovation priorities cannot be high in such an environment. This situation

can cause decline, because without investment in the future and in infrastructure, industries are dying.

For the purpose of carrying out the empirical analysis on the test of the formulated hypotheses, the method of modeling structural equations (MSR) was applied, which is an effective method of quantitative research on implicit theoretical constructions in modern social research in verifying the conformity of theoretical models of existing practice in general. The method of modeling structural equations is a synthesis of such methods as analysis of the confirmation factor and regression, which allows research to be conducted in another direction. In modern management research, MCP methods are used to test hypotheses, as well as to assess the reliability of the presented theoretical design.

The popularity of the MCR method in foreign research in the field of management is due to its ability to take into account erroneous reports or hidden variables. The analysis is based on a system of equations consisting of several parts, and the observed or explicit variables are represented by a certain numerical expression, measured directly.

The structural component reflects the relationship between implicit variables in a simultaneous system of equations. Therefore, the measurement component in the form of an equation estimates the contribution of each explicit variable to the implicit variable.

The MCP method consists of a number of steps, the first of which uses confirmation factor analysis. This analysis confirms whether the theoretical representations are consistent with empirical data.

This study uses the traditional principal component method to determine the factor load levels of each observed variable. Discussing the scientific method, we note that an important task of the IAS method in management research is to reflect the degree of compliance of internal ideas and expectations of respondents to the theoretical a priori design, which is the variable of the internal and external management environment of the enterprise. Based on the subjective assessments of respondents, this method allows us to assess the degree of such compliance and suitability for further analysis of theoretical ideas. In part, this method from this point of view is similar to the method of expert assessments, except that in recognizing the validity of the structure the most important expert is used, and here all opinions are used.

Variables for simulation included issues of organizational culture, digital culture and learning practices that were adapted from the research of scientists (Kuybida et al., 2019). Data collection was conducted via a survey of 75 enterprises. Several methods of information collection were used: online surveys, telephone and personal interviews. The online survey was conducted on a semi-formalized questionnaire. To determine the size of a representative sample, the following parameters were accepted with a probability of 95% confidence interval, or an error of −5%: the total population was 3,183 respondents. For the estimated sample size, 1,500 people were used, and 20 questionnaires were formed and distributed to 75 enterprises. At the initial stage of the statistical survey, 330 questionnaires were incomplete and thus invalid. After this, the validity was 78%, which is a good result.

At the first stage, the structure of interrelation of variables in modeling was investigated, and the factor analysis for the definition of the size of factorial loadings of each variable was carried out.

Factor loads presented in the matrix of components are interpreted in absolute terms – the higher the load, the more the variable correlates with the factor, and the greater the variable due to this factor. The method of basic components allowed us to determine in advance how many factors to take, because their number was unknown. In factor analysis, an important concept is generality – this is the part of the variance of variables which is explained by the main components, i.e., factors, and is calculated by the sum of squares of loads on the line. To do this, we use rotation in factor analysis, where a given rotation is needed to determine the maximum value of a variable for one factor and the smallest for another factor, because it is

important that one variable does not load other factors – it should load only one factor. Thus, the inverted matrix allowed us to determine which variables load each factor, so the load was considered normal from 0.4. The obtained results allowed us to interpret the following: the first factor is loaded with all variables except PERF_10 and DIGITAL_CULT_18.

The Kaiser–Meier–Olkina (KMO) and Cronbach's Alpha test adequacy indicators indicate the adequacy of the results of the factor analysis. This allowed us to understand the most serious factors that prevent businesses from increasing their digitalization. In the field of digital knowledge, the level of awareness of the prospects for the development of various digital technologies is significant. The main initiators of the implementation of the Digital Solutions Project and the existence of a documented strategy of human capital management in the transition to new digital technologies are important in the practice of human capital management.

To determine the impact of factors on the results of the enterprise, a management chart was constructed, with the calculation of standardized coefficients, regression coefficients of the pair between variables, and factors and models of quality indicators.

Obviously, all coefficients were standardized and therefore suitable for comparison. The values of quality indicators or agreement with this model indicate that the significance of the results is acceptable.

Thus, we can discuss a number of results of testing the hypotheses put forward in this study.

Despite expectations, a significant relationship between the level of digitalization and the overall performance of the company was not found. This may be due to the fact that the studied companies are not clearly perceived by specialists and managers of information technology due to the lack of digitalization, and in most cases are not the subject of strategic planning.

Infrastructure companies are more likely to notice a tangible or significant result in such an assessment of efficiency as improving accuracy and quality. The banking sector is more likely to show a significant result in increasing the flexibility of processes, strengthening their focus on customer needs, increasing sales and the emergence of fundamentally new products. The industrial sector of the economy points to the low impact of projects in terms of increasing sales and the emergence of new consumers, as well as the emergence of fundamentally new products, services and opportunities. Enterprises that are at a mature stage of development more clearly indicate the impact of such parameters as reducing resource opportunities, the emergence of fundamentally new products, services and opportunities, the ability to comply with mandatory standards and consumer requirements.

There was no significant link between organizational digital culture and the level of digitization due to the low level of staff involvement in the digital development project. Digitization of business processes will give impetus to the general complexity of all professions, on the one hand, freeing up time for employees to solve more complex and creative tasks. On the other hand, this presents a significant increase in the requirements for their skills. This will lead to a new approach to the division of responsibilities, in contrast to the long-term principle of one person one task: one employee, or a small team. Thus, part of the principles of organizational culture is the ability to work in a team, where employees need to be responsible for a complex process/product or several processes of different profiles. As a result of the increasing penetration of algorithms and computers, digital organizational culture affects the overall efficiency of the enterprise, and a special role is given to awareness of enterprise experts about digital proposals available on the market, the experience of digital projects of other enterprises, the effects they have received, and initiating senior management to implement digital projects.

Existing human capital management practices mainly affect the level of digitization, and employee qualifications are important variables. In companies with a low level of digitalization, in 33% of cases the low qualification of staff is a barrier. Almost twice as often as other companies, companies in the early stages of development face the problem of high-

cost operating systems (82% vs. 41%–45% in other companies). It turns out that if they are different and can be invested in the project, the cost of continuous maintenance of the system for them can be a serious obstacle. Newcomers are limited in the ability to expand digital projects and due to the low level of infrastructure development (71% vs. 38%–45% of other enterprises) (OECD, n.d.).

A significant, stable relationship between the impact of human capital management practices on the overall efficiency of the enterprise was observed, as this indicator is mainly due to other factors, such as the impact of the market and general economic, political, as well as production, financial and investment management factors. However, this is also due to the fact that only 12% of companies have a separate document as a strategy for human capital management in the transition to new digital technologies for the next 5 years. If we add to this the number of enterprises that do not have such a strategy as a separate document, but at least highlighted it in a separate section, we receive a value of 17% (12% + 5%) of enterprises that, in one form or another, have a view towards new digital technologies. Exactly the same number (17%) do not plan to use digital technologies at all for the next 5 years. More than a quarter of enterprises (27%) include the use of digital technologies only in operational planning during the year. Approximately the same (26%) number do not produce digitization in a separate direction or separate section, but take into account the possibility of using digital technologies (either as stand-alone projects – 12% – or long-term investment projects – 14%).

There is a significant lasting impact of digital knowledge on the level of digitalization of the enterprise. Slightly more than one third of respondents (37%) believed that their company's specialists have all the necessary information about the development of digital technologies and are well aware of the degree of their possible impact on the company's business. A quarter of respondents (25%) were less confident in the knowledge of their specialists and their ability to assess the possible impact of digital technologies on the activities of enterprises. Thus, at least 2/3 of respondents (62% in total) provided a sufficiently high level of awareness and competence of their employees to assess the impact of digital technologies on the activities of enterprises.

Conclusions

The digitalization of Ukraine's economy is different from what is happening elsewhere in the world. In Ukraine, digitalization is perceived as the creation of new types of services based on the collection and analysis of data from various physical objects. The directions of radical change of the situation in the production system and approaches to the design, production, sale and operation of these physical objects, which are enshrined in the concept of Industry 4.0, are almost not considered.

The economic effect of the digitalization of industry can be multifaceted, involving: digitalization of technological processes; ways of organizing production; and digitalization of means of labor (equipment, devices, machines), with the best quality characteristics.

In recent years, the digitalization of business has continued rapidly. In all sectors of the economy, businesses of all sizes are increasingly equipping their staff with digital tools, although SMEs are doing so more slowly.

Digitization is multifaceted, as it involves the use of different technologies that serve different purposes and requires the recombination of different strategic assets.

Not all SMEs have the capacity to make this transformation. The smaller firms are, the less likely they are to apply new digital practices, and the more likely they are to limit their consumption of basic services. In general, the digitization of SMEs is closely linked to the way that value is created in the firm and the sector in which it operates.

Business surveys on the use of ICT show that the digital divide is smaller between SMEs and large firms in their online interactions with government, in electronic invoicing, and in the use of social media or the Internet. However, gaps in the use of SMEs widen as technologies become more sophisticated (e.g., data analytics) or massive implementation issues (e.g., enterprise resource planning for process integration) emerge. Firms also have striking differences in the use of cloud technology.

Almost all sectors of the economy are responding to policies to promote the use of digital technologies by businesses. In addition, many highlight policies that support technological progress and the development of innovative products, as well as their adoption. ICT supports the development of the digital economy and makes an increasingly important contribution to the country's economic growth. Digitization makes it easy to store and change information and knowledge. Digital technologies are creating a system of mass media and communication that increasingly connects all parts of social and economic life. This interactivity not only promotes entrepreneurship through digital innovation, but also increases the level of digital security.

The impact of individual components of human capital on the digital and general performance of industrial enterprises was also assessed on the basis of methods of factor analysis and modeling of structural equations. This research was based on the experience of 75 Ukrainian companies.

The study focused on theoretical structures such as digital culture, human capital management practices and digital knowledge of employees. The analysis of human capital management practices showed that only 12% of enterprises have a strategy of human capital management in the transition to new digital technologies for the next 5 years as a separate document. Companies that actively increase the competence of employees in the field of digitization and broadcast and implement the principles of international standards receive business benefits in such areas as reducing resource opportunities, the emergence of fundamentally new products and services, and opportunities to meet the required standards and customer requirements.

Contrary to expectations, there was no significant link between the organizational digital culture and the level of digitization due to the low level of staff involvement in the digital development project, but the digital organizational culture affects the overall efficiency of the enterprise. This involves the experience of the implementation of digital projects by other enterprises regarding these received effects, and also the initiation of top management for the realization of digital projects.

Thus, the issue of the digital security of enterprises and employees is one of the means of minimizing risk. Economic security, which is primarily related to the detection and prevention of fraud, is directly related to cybersecurity and confidentiality (the protection of systems from theft). Today, the use of digital technology is becoming a matter not only for specially appointed IT professionals, but also for all employees of the company, from the CEO to ordinary contractors and workers. Without an understanding of the systemic changes taking place, it will be very difficult for Ukrainian companies to withstand competition in current and future markets.

References

1. Abid, A., & Jemili, F. (2020). Intrusion detection based on graph oriented big data analytics. *Procedia Computer Science*, *176*, 572–581.
2. Ayres, R. U., & Williams, E. (2004). The digital economy: Where do we stand?. *Technological Forecasting and Social Change*, *71*(4), 315–339.
3. Beedham, M. (2019). *All you need to know about bitcoin network nodes*.
4. Canellis, A. (2018). La *Lettre 64* de Saint Jérôme et le symbolisme des couleurs: Les vêtements sacerdotaux d'Exode. *Vigiliae Christianae*, *72*(3), 235–254.

5. Carlsson, B. (2004). The digital economy: What is new and what is not? *Structural change and economic dynamics*, *15*(3), 245–264.
6. *Digital Agenda of Ukraine – 2020*. (2016). http://ucci.org.ua/uploads/files/58e78ee3c3922.pdf
7. Dannikov, O. V., & Sichkarenko, K. O. (2018). Kontseptualni zasady tsyfrovizatsii ekonomiky Ukrainy. *Infrastruktura rynku*, No. 17, 73–80.
8. Ebers, M., & Steinrötter, B. (eds.). (2021). *Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht* (Vol. 1). Nomos Verlag.
9. Fedotova, T. A. (2017). Economic content of labor in the labor market. *Economic Forum*, No. 2, 348–352.
10. Grishnova, O. A. (2014). Human, intellectual and social capital of Ukraine: Essence, interconnection, assessment, directions of development. *Social-labor relations: Theory and practice*, No. 1, 34–40.
11. Gudz, O. E. (2018). Cyfrova ekonomika: zmina cinnostej ta orijentyriv upravlinnja pidpryjemstvamy [Digital economy: Changing the values and guidelines of enterprise management]. *Economy. Management. Business*, 24*(*2), 4–12.
12. Haanaes, K., & Fjeldstad, O. D. (2018). *Which business models are most affected by digital? Four types of businesses where technology is speeding up change*. IMD. https://www.imd.org/contentassets/c18165f15456452f8319682a4fb2d31e/tc071-16_which-business-models-are-most-affected-by-digital_haanaes-fjeldstad_.pdf
13. Il'chenko, A. O. (2021). *Світові тенденції розвитку глобальної цифрової економіки* [World trends in the development of the global digital economy]. https://er.nau.edu.ua/handle/NAU/53987
14. Kharchyshyna, O. V. (2008). Orhanizatsiina kultura yak faktor motyvatsii personalu pidpryiemstva. *Visnyk Derzhavnoho ahroekolohichnoho universytetu*, No. 1, 226–235.
15. Kianto, A., Sáenz, J., & Aramburu, N. (2017). Knowledge-based human resource management practices, intellectual capital and innovation. *Journal of Business Research*, *81*, 11–20.
16. Kolyadenko, S. V. (2016). Digital economy: preconditions and stages of formation in Ukraine and in the world. *Economy. Finances. Management*, *6*, 106–107.
17. Kuybida, V., Petroye, O., Fedulova, L., & Androshchuk, G. (2019). Tsyfrovi kompetentsii yak umova formuvannia yakosti liudskoho kapitalu [Digital Competences as a Condition to the Development of Quality of Human Capital]. *Zbirnyk naukovykh prats Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy*, No. 1, 118–133.
18. Matveychuk, L. O. (2018). Cifrova ekonomika: teoretichni aspekti. *Visnik Zaporiz'kogo nacional'nogo universitetu. Ekonomichni nauki*, No. 4, 116–127.
19. National Bank of Ukraine. (2020). *Macroeconomic and monetary review of the NBU*. http://bank.gov.ua/admin_uploads/article/%D0%9C%D0%9C_2020-02.pdf?v=4
20. National Economic Strategy of Ukraine 2030. (n.d.). https://www.kmu.gov.ua/en/news/denis-shmigal-uryad-zatverdiv-nacionalnu-ekonomichnu-strategiyu-do-2030-roku
21. Netscout. (2019). *Netscout Worldwide Infrastructure Security Report* (Issue 4). Westford, MA: Netscout. http://www.netscout.com/sites/default/files/2020-02/SECR_001_EN-2001_Web.pdf
22. NexusGuard. (2019). *Threat Report: Distributed Denial of Service (DDoS) Q3*. https://www.nexusguard.com/hubfs/Q3%202019%20Threat%20Report/2019Q3_Threat%20Report.pdf
23. OECD. (n.d.). *OECD Digital Economy Papers*. http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826
24. Petrov, A. N. (2019). Sovremennyj strategicheskij menedzhment: ekonomizm ili

sozdanie smyslov? In *Sovremennyj menedzhment: problemy i perspektivy* (pp. 45–56).
25. Schwab, K. (2019). *The Global Competitiveness Report 2019*. World Economic Forum. http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf
26. State Statistics Service of Ukraine. (2018). *Scientific and innovative activity of Ukraine*. http://www.ukrstat.gov.ua/druk/publicat/kat_u/2018/zb/09/zb_nauka_2017.pdf
27. State Statistics Service of Ukraine. (2020). *Economic statistics / Economic activity / Activity of enterprises*. http://ukrstat.gov.ua/operativ/menu/menu_u/sze.htm
28. Symantec. (2019). *Internet security threat report: Volume 24*.
29. The World Bank. (n.d.). *GDP per capita (current US$) – Ukraine*. http://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=UA
30. Yarova, L. H. (2015). Analysis of unemployment in Ukraine and ways of its overcoming. *Hlobalni ta natsionalni problemy ekonomiky*, No. 4, 752–755.