https://doi.org/10.38104/vadyba.2023.2.03

Vadyba
Journal of Management
2023, № 2 (39)
ISSN 1648-7974

DIGITAL TECHNOLOGIES AS A FACTOR OF NATIONAL SECURITY OF UKRAINE

Anna Zadorozhna
Ivan Franko National University of Lviv

Abstract
Digitalization has a significant impact on the sovereignty of the state and its national security. In its turn, national security determines the measures and requirements that apply to the informatization of society and information security. The relationship between national security and digitalization means that one cannot talk about national security without taking into account the degree of digitalization of the country. The problems of digitalization of Ukraine has been researched by many authors. However, it takes on special significance now that national security is becoming especially important for the country. The purpose of the study is to estimate the state of digital development of Ukraine and the cyber threats that the country has experienced and formulate basic recommendations for the further digital development of Ukraine. The author examines the issue of digitalization from the point of view of strengthening Ukraine's position on the world stage, and those dangerous moments of digitalization that may appear in the case of military aggression. The author analyzes various indicators of digitalization as well as the state's contribution to the development of information and communication technologies. In particular, Ukraine improved its position according to the generalized indicator of the level of development of information and communication technologies NRI from 71st place in 2015 to 50th place in 2022. Calculations showed that in recent years the state did not allocate enough budget funds to the field of information and communication technologies. A different situation is observed for the private sector in 2019–2021 – the share of capital investments from internal sources of enterprises and organizations in the "Information and Telecommunications" section exceeds the average level of capital investments disbursed from such sources in the whole economy. The downside of digitalization is the increase in cyber attacks with the spread of information and communication technologies. The work examines those examples of cyber attacks that Ukraine has experienced since the beginning of Russian aggression. In the context of hostilities, Ukraine needs to increase the level of cyber protection, because the country is not among the top ten countries in the world with the highest GCI score.
Keywords: digitalization, digital economy, national security, cybersecurity, capital investment, Internet, digitization development indicators, new economy.

Introduction

National security is a broad concept that means a set of measures to ensure and preserve the nation. Every nation that wants to preserve its identity, its culture and the territory on which it has formed a state must pay significant attention to ensuring national security. National security is one of the required factors for the existence of a state. It ensures stability in the existence of the state and society, promotes their gradual development by preventing, identifying and neutralizing threats to the state.

In today's world, digitalization has an impact on all areas of social development. It determines the progress of the state's development, including in the economic sphere. Active implementation of information and communication technologies promotes to long-term growth of the national economy, increasing the level of public administration, and improving health and education.

The widespread use of digitalization also affects the sovereignty of the state, its national security. In its turn, national security determines the measures and requirements that apply to the informatization of society and information security. Without a national policy for organizing the protection of information resources, there can be no national security. Therefore, national security and digitalization are interconnected.

Information security is of particular importance and can have a significant impact on the military security of the state and its existence as a whole. This is due to the development and active use of innovative technologies and modern information systems in human activity, and the acquisition by an information resource of the role of a strategic resource of the country.

In a broad sense, information security is a set of measures aimed at ensuring the security of information from unauthorized access, use, disclosure, destruction, modification, review, inspection, recording or destruction.

A new stage in the development of information security can be called cybersecurity, which in a simplified formulation can be defined as the security of an exclusively digital environment. The goal of cybersecurity is to develop and use methods and practices to protect digital data, networks, computer systems, servers, software and hardware, and mobile devices from intruders.

The purpose of the work is to analyze the state of digital development of Ukraine and the cyber threats that the country has experienced and formulate basic recommendations for the further digital development of Ukraine.

The object of research is digital technologies. The subject of the study is the impact of digital technologies on national security.

Literature Review

The role of technology in the development of a society, changes in the development cycles of productive forces over a significant period of time were studied in (Melnyk, Dehtyarova, et al., 2019), where the positive and negative features of the implementation of disruptive technologies were noted. The work emphasized that digital technologies are one of the factors that improve economic development.

Many publications are devoted to the problems of the emergence and development of the "new" economy, the peculiarities of its formation. The authors (Dziatkovskii, Hryneuski, et al., 2021; Gobble, 2018) investigate the principles of digitalization of the economy and emphasize the need to attract both public and private investment in the digital economy also. According to the authors, the position of the state is important – the development of specific measures of state support of the economy digitalization.

General questions of business process management in the context of digital transformation were studied in (Stjepić, et al., 2020). It is indicated, that digitalization is more focused on customers who require high quality of services offered. The need for greater process flexibility leads to the appearance of new business models in organizations.

According to V. Koibichuk, N. Ostrovska (2021), the use of digital communication platforms for making purchases on the Internet is of particular importance. R. Bacik et al. (2020) showed that today's consumers prefer to make purchases on the Internet, in particular, using mobile devices. By using digital channels of communication with consumers in their activities, businesses can increase the level of profitability (Bacik, et al., 2020).

Some authors note that attention needs to be paid to the security and protection of consumer data when digitalizing business processes (Skrynnyk, 2020). At the same time, the digitalization process is considered as one of the most important areas of managing the development of an organization. This aspect also examines the impact of innovative information and communication technologies on employee performance (Alyoubi, Yamin, 2019).

In particular, the authors evaluate the advantages and disadvantages of ICT for organizations. G. Pajtinkova Bartakova, K. Gubiniova et al. (2017) assessed the potential and ease of use of social networks for employers – representatives of small and medium-sized businesses. The authors showed that the use of digital technologies makes it easier for SMEs to recruit staff through social networks. The issues discussed in our article are also, to a certain extent, related to the articles by Yanyshyn (2019) and Yu. Harust (2019).

Studying the creation of value for customers in the case of small businesses (using the example of the fashion, furniture and food industries), the authors (Matarazzo, Penco, et al., 2021) concluded that neglecting of digitization in the work of medium and small businesses can cause bankruptcy and closure of companies. They have shown, that digital transformation causes a change in the business model and customer value creation processes.

The problem of the correct organization of financial security is considered in the work (Koibichuk, Dotsenko, 2023). A group of clusters has been formed that characterizes their methods and technologies for detecting cyber threats. This allowed the authors to provide comprehensive recommendations for organizing cybersecurity in financial institutions, as well as note the annual growth of the global cybersecurity market.

According to the authors (Simonavičiūtė, Navickas, 2022), the digitalization of business strongly depends on the general level of digitalization of the country. The latter depends on various factors, including financial investments in network infrastructure. The authors of (Simonavičiūtė, Navickas, 2022) found problematic points in the digitalization of Lithuania and noted the importance of achieving a high level of connectivity (5G) in the country.

The importance of a high level of communication (5G) is shown in work (Akpan, Ibidunni, 2021), where the influence of various generations of network technologies up to and including 5G on the rate of industry digitization and intelligent automation was studied. It is indicated, what opportunities can be provided by 5G communication for the further development of various industries, including smart industries, IoT, automobiles, smart cities and healthcare.

The need for comprehensive digitalization and implementation of ICT, the ability to use IT skills imposes its requirements on the development of society and its education. Thus, in work (Éva Görgényi Hegyes, et al., 2017), using the example of Hungary, the importance of developing of digital skills for the further development of the country's "new economy" is shown.

One of the factors that determine the success of the implementation of digital technologies and the development of society and the country in general is the level of human development. The latter takes into account many components – literacy level, life expectancy, standard of living. To find the Human Development Index (HDI), for example, a mathematical-statistical method is used, as in (Masárová, Husárová, 2013). A more detailed analysis of the role of human capital in the development of the economy and society in the context of information technologies is contained in (Vojtovič, Karbach, 2014). In the context of the global digitalization of all spheres of life, the authors (Vojtovič, Karbach, 2014) pay considerable attention to the problems of digitalization of Ukraine.

Attempts to estimate the quality of life in Ukraine were made in (Boronos, Plikus, et al., 2018), where the authors proposed a model for the digital transformation of the economy and society. Having decomposed the digital space into three components – business, education and science, state and society, the authors monitored the readiness of the components for digital changes and the use of information and communication technologies. Using this methodology, it is shown that in 2015 Ukraine lagged significantly behind in digital quality of life.

An assessment of the prospects that digital technologies can provide is made in (Pecheranskyi, Revenko, 2019). The authors focus on attempts to

overcome the post-Soviet past and make a technological breakthrough. To do this, the authors analyzed the experience of using advanced information and communication technologies in the digital economy of the advanced countries of the world. They recommend to create a technological infrastructure, teach digital skills and information security to personnel, create digital platforms and develop a legal framework. In this context, the work (Kaminsky, Korzachenko, et al., 2017) is of interest, in which the prospects for creating an innovative public cloud platform are considered, which will allow Ukraine to provide all government services and innovative services.

A comparative analysis of the level of digitalization and its impact on the economies of Ukraine and Poland was carried out in (Melnyk, Shchehliuk, et al., 2021). Research results indicate the strong impact of digitalization on economic growth and innovation. The work suggests ways to improve digitalization - invest more in the development of the information and telecommunications infrastructure of the regions, reduce the gap between the rural and urban populations. Great importance is also attached to the human factor – the growth of digital literacy of the population, as well as cybersecurity.

A study of the state of digitalization of Ukraine was also carried out in (Samoilovych, Garafonova, et al., 2021). It emphasizes the need for systemic action from the state.

In order to increase the level of digital skills and ensure high-quality human capital, significant attention must be paid to education. This problem is discussed in article (Djakona, Kholiavko, et al., 2021), where, using the example of Latvia, the influence of higher education on the dynamics of the information economy is studied and recommendations are given for the further digitalization of Ukraine.

The authors of work (Sembekov, Tazhbayev, et al., 2021), dedicated to digital modernization in Kazakhstan, also come to conclusions similar to those in (Samoilovych, et al., 2021; Djakona, et al., 2021). They link the development of the digital economy with the availability of digital communications, the development of digital literacy and the level of e-government.

Methodology

In order to estimate the level of digitalization of the economy, data from the State Statistics Service of Ukraine was used. The volumes of capital investments and their share in the Ukrainian economy as a whole and in the section “Information and telecommunications” have been calculated. Data on the Networked Readiness Index (NRI) were taken from the website of the Portulance Institute, an independent, non-professional, non-specialized research and educational institute based in Washington DC (Portulance Institute).

The use of information and communication technologies determines cybersecurity questions. The latter is closely related to the secrecy of information, especially during hostilities. However, some of the data on cyber attacks was made public on the CyberPeace Institute website, which tracks cyber attacks in times of conflict. In addition, data from the Statista website was used as well as an official information about cybercrimes against Ukraine and attempts to prevent them.

Research Results

The digital economy refers to an economy that depends on ICT. In particular, in order to estimate the state of informatization of the country and the economy, some e-indices can be used. We will consider the Networked Readiness Index (NRI) – a generalized indicator that characterizes the level of ICT development in the countries of the world. The advantage of NRI is that it is calculated on the basis of 64 different assessments, and therefore it quite comprehensively reflects areas such as “Technology”, “People”, “Governance”, “Impact”.

Ukraine is improving the value of the Networked Readiness Index and continues to increasingly introduce network and digital technologies into its economy. According to data (Portulance Institute), Ukraine rose from 71st place in 2015 to 50th place in 2022 in terms of ICT influence (by network readiness).

Table 1. The Network Readiness Index (NRI) of Ukraine (100 = Best)

Year	Rank	Score	Total number of countries	Technology	People	Governance	Impact
2019	67	48.92	121	43.01	42.05	58.32	52.31
2020	64	49.43	134	41.51	48.87	58.19	49.16
2021	53	55.70	130	49.20	54.29	58.93	60.40
2022	50	55.71	131	50.52	54.43	60.81	57.08

Source: Portulance Institute

To analyze the state policy of Ukraine regarding the spread of information and communication technologies, let’s turn to the statistical data on the volume of capital investments by sources of financing (by types of economic activity) (Table 2) (State Statistics Service of Ukraine).

As it can be seen, in 2020–2021 capital investments were financed from budget resources in the amount of 19 % and 18 % of their total volume, respectively (from all sources of financing), as opposed to 2018–2019 (13 % and 14 % respectively). At the same time, the share of budget capital investments in the “Information and Telecommunications” section for 2020 is more than 6 times lower (2.7%) with the share of budget financing of capital investments in the economy as a whole (19 %). And only in 2021 the situation becomes the same as in 2019 – the share of budgetary capital investments in the section “Information and telecommunications” is 3 times

less (4.8 %) than the share of budgetary financing of capital investments in general economy (18 %). For these purposes, in 2020–2021 the share of capital investments amounted to 67.0 and 68.6% of the total costs at the expense of internal enterprises and organizations (non-budgetary expenses).

As can be seen in table 2, the share of capital investments from internal sources of enterprises and organizations (non-budgetary funds) in the section "Information and telecommunications" in 2020–2021 exceeds the average level of capital investments disbursed from such sources in the economy (85 and 83% versus 67 and 68.6% respectively).

Table 2. Volumes and structure of capital investments by sources of financing in the economy of Ukraine and in the section "Information and telecommunications" in 2019–2021

Years	Code	Total used capital investments, billion UAH	Including at the expense		Share of capital investments from budget funds	Share of capital investments from internal sources of enterprises and organizations (non-budgetary funds)
			budget funds	own funds of enterprises and organizations (non-budgetary funds)		
2019	in general for the economy	624.0	87.3	408.3	14 %	65 %
	in the section "Information and telecommunications"	21.1	0.80	18.4	4 %	87 %
2020	in general for the economy	419,8	80.1	279.3	19 %	67 %
	in the section "Information and telecommunications"	21.1	0.57	17.85	2.7 %	85 %
2021	in general for the economy	528.8	92.8	362.7	18 %	68.6 %
	in the section "Information and telecommunications"	20.1	0.96	16.7	4.8 %	83 %

Source: calculated from the data (Website of the State Statistics Service of Ukraine)

Using the data in table 3, we can conclude that the share of capital investments in the "Information and Telecommunications" section in the structure of capital investments in the economy in 2020-2021 was 5.0 and 3.8%, respectively. At the same time, enterprises and organizations allocated 6.4 and 4.6% of the total amount of financial resources that were allocated for capital investments in the respective years to capital investments in the "Information and Telecommunications" section at the expense of their own funds, while only 0.7 and 1.0 % were allocated from budget funds respectively.

Up to 90% of enterprises in Ukraine have access to the Internet (Table 3), while only 10 % of enterprises use cloud computing services. The authors (Pecheranskyi, Revenko, 2019; Kaminsky, et al., 2017) pointed out the same problem when they noted the need for more active use of cloud platforms in Ukraine.

An important priority for digital transformation is digital inclusion, so that all citizens can use government electronic services without limitation. The increased level of digitalization also means more active and simplified interaction between communities and government authorities, for which the e-Government system has been introduced in Ukraine. Despite the fact, that Ukraine belongs to the category of European countries with lower middle income, since 2012 it has gone from an average level of EGDI to a very high E-Government Development Index.

Table 3. The use of information and communication technologies at enterprises of Ukraine by types of economic activity (% of the total number of enterprises)

Type of service	2018	2019	2021
access to the Internet	88	86.4	86.6
website	35.6	35.2	35.3
cloud computing services	9.8	10.3	10.2

Source: Website of the State Statistics Service of Ukraine.

As can be seen from Table 4, it was the high Human Capital Component that ensured the average and high value of EGDI in 2014–2018. From 2020 there is a significant increase in the Online Service Component, and the telecommunication infrastructure is also improving (up to 0.727), which allows to estimate the level of EGDI as very high.

At the same time, when talking about digitalization, one should not forget about its reverse side - the increase in the number of cyber attacks with the spread of information and communication technologies. A lot of attention is devoted to the problem of studying of the development peculiarities and trends of cyber security. In particular, a generalized Global Cybersecurity Index (GCI) was introduced to estimate the level of cyber security of countries. It includes legal, technical and organizational measures to ensure cyber security, and also takes into account such indicators as building of the potential of the state and its international cooperation.

Table 4. E-Government Index of Ukraine

Year	Rank	EGDI level	EGDI	Online Service Component	Telecomm. Infrustructure Component	Human Capital Component
2014	87	middle	0.5032	0.2677	0.3802	0.8616
2016	62	high	0.6076	0.5870	0.3968	0.8390
2018	82	high	0.6165	0.5694	0.4364	0.8436
2020	69	high	0.7119	0.6824	0.5942	0.8591
2022	46	very high	0.9211	0.8148	0.7270	0.8669

Source: Unated Nations: Department of Economic and Social AffairsPublic Institutions

According to the report (Statista), the United States has the highest level of cybersecurity in the world in 2020 (GCI=100), the second and third places are occupied by the UK and Saudi Arabia, respectively, and Estonia is in fourth place. It should be noted, that the list of 10 countries with a high GCI rating includes countries from the East and Asia also. As for Ukraine, in 2020 it did not enter the top ten countries in the world with the highest GCI index. At the same time, it would be incorrect to claim that Ukraine does not take sufficient measures to guarantee its cyber security. Thus, the level of protection of management system of Ukraine's power system at the time of the 2015–2016 attacks was at such a level that it required cybercriminals to prepare for a long time and implement a multi-stage action plan.

The cybersecurity situation in Ukraine has become especially important since the proclamation of the anti-terrorism operation (ATO) and has become critically significant since the full-scale aggression of Russia.

The effectiveness of cyber attacks is evidenced by the failure of the Ukrainian energy system in 2015 and 2016. Then, within six hours, many users were de-energized using a whole system of measures. This was preceded by complex and lengthy preparation for a massive attack:

– infection of computer networks of energy companies;

– intervention in work of automated distance control systems;

– development of malicious programs and replacements of industrial programs with them;

– destruction of information on servers used by energy companies;

– disabling call centers for customer service.

As the leadership of the Cybersecurity and Infrastructure Security Agency (CISA) notes, attacks on the digital space of Ukraine were carried out in several directions simultaneously – the spread of malicious software, DDoS attacks and attacks on websites (Fedorov).

The fact that cyberspace can become one of the theaters of military operations, the criminality of the Russian Federation's intentions was stated in Decree of the President of Ukraine No. 447/2021 of May 14, 2021: "The Russian Federation remains one of the main sources of threats to national and international cybersecurity, and is actively implementing the concept information warfare based on a combination of destructive actions in cyberspace and information and psychological operations, the mechanisms of which are actively used in the hybrid war against Ukraine. Such a destructive activity creates a real threat of acts of cyberterrorism and cybersabotage against the national information infrastructure". The same Decree contained a list of challenges and threats to Ukraine's cybersecurity, outlined the range of tasks for the further development of the national cybersecurity system, noted the priorities for ensuring it and the country's strategic goals.

As the events of the beginning of 2022 showed, this prediction of Russia's aggressive actions, including in the cyber direction, turned out to be correct. Even before the beginning of the large-scale invasion, from January 13, 2022, repeated attacks were carried out on Public administration (Campaign: Defacement of Ukraine Government Websites, Attempt to Compromise a Foreign Government Entity), ICT, nonprofit attacks (CyberPeace Institute).

Only within 6 months of the start of the large-scale invasion, Ukraine suffered 1123 hacker attacks and continues to experience them further. In particular, on the night of February 23-24, 2022, Russia attacked and disabled the sectors of energy, transport, education, medicine, government, public administration, and finance. The websites of the Ministry of Defense of Ukraine were also subject to aggressive hacker actions (CyberPeace Institute).

On February 25, Russia carried out DDoS attacks on news sites (media) and government administration, websites of Ukrainian universities were broken, and cyber attacks on border control points were continued. Civilian users became targets of aggressive actions also, for example, SunSeed and other malicious software were distributed, and disinformation was occurred on the social network Facebook. All these acts were designed to disable the main political, military and social institutions of the country, to cause panic and disorientation of authorities, organizations and people.

Investigations based on intelligence data from the UK, EU and Canada allowed the EU to gather evidence and accuse Russia of deliberately cyberattacking Ukraine's satellite network an hour before the full-scale invasion, which affected the infrastructure and users not only of Ukraine, but also of other countries. Thus, we can state that in the modern world, a military invasion of another country is necessarily accompanied by an attempt to invade its cyberspace, launching information attacks and disabling the country's main infrastructure.

The fact that cyber security is important for the security of the country is also confirmed by the efforts of the Russian Federation to attack the energy system of Ukraine in October 2022 not only with missile attacks, but also with massive cyber attacks on critical infrastructure facilities, with the aim of complicating the counteroffensive of the Ukrainian armed forces.

Assessing the danger of cyberattacks from the Russian Federation, the European Union decided to allocate 29 million euros to strengthen countermeasures against threats in cyberspace and digital space of Ukraine, and held consultations on countering hostile attacks also. At the same time, the scale of the Russian aggression may reach such a level that DDoS attacks will be attempted on the critical infrastructure of those EU countries that support Ukraine in the war of liberation and are its allies. Periodically, statements appear from various allies of Ukraine about Russia's attempts to attack and harm one or another of their industries. The Government of Ukraine, in its turn, by the Law of Ukraine "On Amendments to Certain Laws of Ukraine to Ensure the Formation and Implementation of State Policy in the Sphere of Active Counteraction to Aggression in Cyberspace" (No. 2470-IX dated July 28, 2022) granted additional powers to the State Special Communications Service.

The latter signed an international memorandum on cooperation in the field of cyber security with the Cybersecurity and Infrastructure Security Agency (CISA) of the US Department of National Security. Threats to digital security, which EU countries have observed on the example of Russia's aggression against Ukraine, force them to pay more attention to cyber security. An example is Slovenia, which recently signed a memorandum of understanding with Ukraine in the field of cyber security and information protection.

Today, more than ever, Ukraine needs to take all measures to counter cyberattacks for its sovereign future. Such counteraction will be effective only under the conditions of an integrated approach and requires comprehensive assistance from the state.

Conclusions

An analysis of Ukraine's digital development showed that it improved its position according to the generalized NRI e-indicator. In particular, it moved from 71st place in 2015 to 50th place in 2022 and continues to increasingly incorporate networked and digital technologies into its economy.

As the study showed, the state is insufficiently financing the digitization process - the share of budget capital investments in the "Information and Telecommunications" section is 3 times less than the share of budget financing of capital investments in the economy as a whole in 2021. The opposite situation was observed for private enterprises. However, there is a problem that previous researchers have already emphasized. Despite the high level of Internet access, only a third of enterprises have websites, and only 10 % use cloud computing platforms. The state should pay more attention to the financing of the "Information and Telecommunications" section.

Among the advantages of Ukraine is the achievement of a very high level of EGDI indicator (0.9211) for the first time in recent years. It should be noted that if before 2022 Ukraine had a high level of EGDI, primarily due to the high value of the Human Capital Component, then in 2022 the Online Service Component (0.8148) and the Telecommunication Infrustructure Component (0.727) also showed high values.

Unfortunately, Ukraine lags behind the leading countries in the world in cybersecurity level. So, if in 2015–2016 Ukraine provided a high level of protection for the energy system management system, then a different situation occurred in February 2022. A massive attack on the country's digital infrastructure by the Russian Federation was carried out on all state websites of Ukraine – websites of the energy, transport, education, medicine, government, public administration, finance, the Ministry of Defense on the first day of the war.

It is obvious, that countering massive enemy cyber attacks requires a comprehensive approach and support from the state. Further development of digital technologies will allow Ukraine to improve the state of its economy, accelerate social development, and strengthen national security.

References

Akpan, I. J., & Ibidunni, A. S. (2021). Digitization and technological transformation of small business for sustainable development in the less developed and emerging economies: a research note and call for papers. *Journal of Small Business & Entrepreneurship*, 1–7. https://doi.org/10.1080/08276331.2021.1924505

Alyoubi, B. A., Yamin, M. A. Y. (2019). The impact of task technology fit on employee job performance. *Marketing and Management of Innovations*, 4, 140–159. https://doi.org/10.21272/mmi.2019.4-12

Bacik, R., Gavurova, B., Fedorko, R., & Olearova, M. (2020). Using digital devices in the process of online shopping: a study of demographic differences. *Marketing and Management of Innovations*, 4, 154–167. https://doi.org/10.21272/mmi.2020.4-12

Boronos, V., Plikus, I., Aleksandrov, V., & Antoniuk, N. (2018). Digital transformation of Ukraine: challenges of theory and practice in implementation of digital quality of life. *Economic Annals-XXI*, 172(7–8), 38–43. https://doi.org/10.21003/ea.V172-07

Countries with the highest commitment to cyber security based on the Global Cybersecurity Index (GCI) in 2020. https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/

CyberPeace Institute. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

Djakona, A., Kholiavko, N., Dubyna, M., Zhavoronok, A., & Fedyshyn, M. (2021). Educational dominant of the information economy development: a case of Latvia for Ukraine. *Economic Annals-XXI*, 192(7–-8(2)), 108–124. https://doi.org/10.21003/ea.V192-09

Dziatkovskii, A., Hryneuski, U., Dudov, A., & Krylova, A. (2021). The economic impact of digitalization and the creation of digital products on the development of the state. *Economic Annals-XXI*, 193(9-10), 4–14. https://doi.org/10.21003/ea.V193-01

Éva Görgényi Hegyes, Ildikó Csapó, I., Mária Fekete Farkas. (2017). Some aspects of digitalization and sustainability in the European Union. *Journal of Management*, 2(31), 37–46.

Fedorov. https://www.ukrinform.ua/rubric-technology/3568970-hakeri-fsb-atakuvali-ukrainu-za-piv-roku-do-povnomasstabnoi-vijni-fedorov.html

Gobble, M. M. (2018). Digitalization, digitization, and innovation. *Research-Technology Management*, 61(4), 56–59. https://doi.org/10.1080/08956308.2018.1471280

Harust, Yu., Melnyk, V. (2019). Economic security of the country: marketing, institutional and political determinants. *Marketing and Management of Innovations*, 4, 373-382. https://doi.org/10.21272/mmi.2019.4-29

Kaminsky, O., Korzachenko, O., & Samchenko, N. (2017). Cloud computing concept in Ukraine: a study of innovative development. Economic Annals-XXI, 167(9–10), 28–31. doi: https://doi.org/10.21003/ea.V167-06

Koibichuk, V., Dotsenko, T. (2023). Content and Meaning of Financial Cyber Security: a Bibliometric Analysis. *Financial Markets, Institutions and Risks*, 7(1), 145–153. https://doi.org/10.21272/fmir.7(1).145-153.2023

Koibichuk, V., Ostrovska, N., Kashiyeva, F., & Kwilinski, A. (2021). Innovation technology and cyber frauds risks of neobanks: gravity model analysis. *Marketing and Management of Innovations*, 1, 253–265. https://doi.org/10.21272/mmi.2021.1-19

Masárová, T., Husárová, I. (2013). Prognosis of human development index (hdi) of Slovak Republic. *Journal of Management*, 2(23), 149–154.

Matarazzo, M., Penco, L., Profumo, G., & Quaglia, R. (2021). Digital transformation and customer value creation in Made in Italy SMEs: A dynamic capabilities perspective. *Journal of Business Research*, 123, 642–656. https://doi.org/10.1016/j.jbusres.2020.10.033

Melnyk, L., Dehtyarova, I., Kubatko, O., Karintseva, O., & Derykolenko, A. (2019). Disruptive technologies for the transition of digital economies towards sustainability. *Economic Annals-XXI*, 179(9-10), 22–30. doi: https://doi.org/10.21003/ea.V179-02

Melnyk, M., Shchehliuk, S., Leshchukh, I., & Litorovych, O. (2021). Digitalization of the economies of Ukraine and Poland: national and local dimensions. *Economic Annals-XXI*, 191(7–8(1)), 30–42. doi: https://doi.org/10.21003/ea.V191-03

Pajtinkova Bartakova, G., Gubiniova, K., Brtkova, J., & Hitka, M. (2017). Actual trends in the recruitment process at small and medium-sized enterprises with the use of social networking. *Economic Annals-XXI*, 164(3–4), 80–84. doi: https://doi.org/10.21003/ea.V164-18

Pecheranskyi, I., & Revenko, A. (2019). Disruptive digital technologies as a means for destroying the foundations of oligarchomics: world experience and challenges for Ukraine. *Economic Annals-XXI*, 179(9–10), 31–39. doi: https://doi.org/10.21003/ea.V179-03

Portulance Institute. https://networkreadinessindex.org/

Samoilovych, A., Garafonova O., Popelo, O., Marhasova, V., & Lazarenko, Y. (2021). World experience and ukrainian realities of digital transformation of regions in the context of the information economy development. *Financial and Credit Activity: Problems of Theory and Practice*, 38(3), 316–325. https://doi.org/10.18371/fcaptp.v3i38.237462

Sembekov, A., Tazhbayev, N., Ulakov, N., Tatiyeva, G., & Budeshov, Ye. (2021). Digital modernization of Kazakhstan's economy in the context of global trends. *Economic Annals-XXI*, 187(1–2), 51–62. doi: https://doi.org/10.21003/ea.V187-05

Simonavičiūtė, P., Navickas, V. (2022). The Features of Business Digitization Development Indicators in Selected Economies. *Journal of Management*, 2(38), 87–94. https://doi.org/10.38104/vadyba.2022.2.08

Skrynnyk, O. (2020). Some aspects of information security in digital organizational management systems. *Marketing and Management of Innovations*, 4, 279-289. https://doi.org/10.21272/mmi.2020.4-23

State Statistics Service of Ukraine. https://ukrstat.gov.ua/operativ/open_data/open_datai.htm

Stjepić, A.-M., Ivančić, L., & Suša Vugec, D. (2020). Mastering digital transformation through business process management: Investigating alignments, goals, orchestration, and roles. *Journal of Entrepreneurship, Management and Innovation*, 16(1), 41–74. https://doi.org/10.7341/20201612

Sutherland, W., Jarrahi, M. H. (2018). The sharing economy and digital platforms: A review and research agenda. *International Journal of Information Management*, 43, 328–341. https://doi.org/10.1016/j.ijinfomgt.2018.07.004

Vojtovič, S., Karbach, R. (2014). New Economy and the development of creative industry. *Journal of Management*, 2(25), 139–143.

Yanyshyn, Y., Bryk, H. & Kashuba, Y. (2019). Problems and perspectives of internet-insurance in Ukraine. *Marketing and Management of Innovations*, 4, 31–38. https://doi.org/10.21272/mmi.2019.4-03

LEGISLATION

On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine № 447/2021. https://zakon.rada.gov.ua/laws/show/447/2021#Text

Decree of the President of Ukraine No. 447/2021 of May 14, 2021

Law of Ukraine "On Amendments to Certain Laws of Ukraine to Ensure the Formation and Implementation of State Policy in the Sphere of Active Counteraction to Aggression in Cyberspace" (No. 2470-IX dated July 28, 2022)

RECEIVED: 28 August 2023 **ACCEPTED: 08 September 2023** **PUBLISHED: 06 October 2023**

Anna Zadorozhna, associate professor in the Department of Digital Economy and Business, Ivan Franko National University of Lviv, Ukraine. Field of Scientific research: information technologies and systems, economic and mathematical modeling of economic processes and phenomena, securities market. Address: St. Kopernyka 3, Lviv, 79000, Ukraine. E-mail: an_zador@ukr.net. ORCID: 0000-0002-9258-1679