This study focuses on refining conceptual approaches to ensuring state economic security, taking into account the trigger points of influence within the information component amid rapid digital development. The research addresses the pressing need for safeguarding the national economy's information security, resilience, and adaptability to digital risks and threats.

The findings indicate that risks and threats within the information space cause substantial financial losses to national economic systems, estimated at over USD 4 billion annually. Given this context, the study substantiates the necessity of a two-tiered proactive approach to economic security at the national level, with a strong emphasis on cybersecurity. The results demonstrate a significant direct correlation between the level of economic digitalization and cybersecurity, with approximately 49.1 % of the variation in a country's cybersecurity level attributable to differences in digital development. The study reveals that some countries prioritize cybersecurity even at early stages of digitalization, while others first advance digital technologies and subsequently focus on securing them. The study identifies trigger points at which information security influences state economic security. The research proves that integrating security aspects of economic and information processes requires the formation of a security-oriented information environment for the national economy to proactively ensure state economic security. The practical value of research results is their potential application for reforming state economic policy in the context of digitalization and ensuring economic security at all levels of the social hierarchy (state, business, individual, society)

Keywords: economic security, digital development, information security, security-oriented information environment

UDC 330.46:004.056
DOI: 10.15587/1729-4061.2024.319256

IMPROVING CONCEPTUAL APPROACHES TO ENSURING STATE ECONOMIC SECURITY UNDER CONDITIONS OF DIGITALIZATION

Oleksandra Maslii
Corresponding author
PhD, Associate Professor*
E-mail: masliioa02@gmail.com
Alona Buriak
PhD, Associate Professor
Department of International Economic Relations and Tourism**
Alina Chaikina
PhD, Associate Professor
Department of Management and Logistics**
Anna Cherviak
PhD, Senior Researcher*
*Department of Finance, Banking and Taxation**
**National University «Yuri Kondratyuk Poltava Polytechnic»
Pershotravnevyi ave., 24, Poltava, Ukraine, 36011

Received 03.10.2024
Received in revised form 25.11.2024
Accepted 10.12.2024
Published 28.02.2025

How to Cite: *Maslii, O., Buriak, A., Chaikina, A., Cherviak, A. (2025). Improving conceptual approaches to ensuring state economic security under conditions of digitalization. Eastern-European Journal of Enterprise Technologies, 1 (13 (133)), 35–45. https://doi.org/10.15587/1729-4061.2024.319256*

1. Introduction

According to various estimates, the growth of the digital economy is more than half of the world's GDP. It includes not only the IT sector but also all economic activity that is ensured by the use of information and communication and other digital technologies, electronic commerce, online services, and the results of activities of digitalized enterprises. The undeniable advantages of using digital technologies are primarily associated with significant potential for innovation, increased labor productivity, and acceleration of business processes in all sectors of the national economy. All this, as well as accelerating and facilitating access to information as a key resource of the digital economy, definitely stimulates economic growth. However, rapid digital transformation, despite numerous advantages, makes the national economy vulnerable to hacker attacks, and the destruction of digital infrastructure or its analog components could cause significant damage to the national economy and the economic security of the state.

The total digitalization of socio-economic relations generates a number of challenges, risks, and threats to the economic security of the state, related to ensuring the confidentiality and security of data. The stability, sustainability, and development of the national economy, financial support to the digital transition, and the economic security of financial institutions primarily depend on the reliability of information protection systems. In addition, the regulatory effectiveness of proactive state management of the processes of ensuring economic security at the macro, meso, micro, and nano levels plays an important role. The complexity of implementing the outlined tasks is due to the synergistic effect of traditional and digital threats, the latter of which are mostly beyond the control or monitoring of state institutions. At the same time, for the national economy of Ukraine with a significant number of systemic disproportions, the challenges of digitalization are catalysts of real threats to economic security. They could cause significant damage and create obstacles to the development of the digital economy and the implementation of national economic interests.

The conceptual basis of the safe development of the national economy under the conditions of Industry 4.0 and Industry 5.0 is information security at all levels of the social hierarchy. The integration of security aspects of economic and information processes requires the transition of the system of security-oriented management of the national econo-

my to a qualitatively new level. This will make it possible to build a reliable digital economy ecosystem and in practice minimize the destructive impact of digital risks and threats. The dominant influence of destructive security factors in the digital domain actualizes the need for an in-depth study of information and economic security under the conditions of digital transformation.

2. Literature review and problem statement

Our bibliometric review of related studies (using VOSViewer, SciVal tools) has demonstrated that the problems of ensuring economic and information security and minimizing digital threats are the subject of increased attention by scientists. In work [1], the problem of ensuring the economic security of the state under the conditions of global challenges is investigated. A model of reintegration of the economic order is proposed, taking into account the requirements of national security. But the issues of information security of the national economy under the conditions of digital transformation of socio-economic relations remained unresolved. In contrast, study [2] determined the place of economic cyber security in the national security system but did not take into account the trigger points of digitalization. Paper [3], based on the results of the study of cyber attacks and other digital threats proved that, taking into account the rapid dynamics of modern transformational processes, a complex set of countermeasures with an emphasis on the key factors of influence is necessary. However, the work does not take into account the principles of economic security for the formation of conceptual approaches to its provision in accordance with modern security requirements.

In general, the task of ensuring the information security of the national economy against risks and threats under the conditions of digital transformation acquires special importance in connection with the growth of geopolitical contradictions under the conditions of Industry 4.0 and 5.0. Thus, in work [4] it is noted that cyber security goes beyond traditional information security, including the protection of not only information resources but also other assets, including the person under conditions of total digitalization. However, the authors of the work do not investigate the hybrid tools of the destructive impact of digitalization. Instead, the author of work [5] proves that cyber attacks in the digitalized world have turned into tools of hybrid wars and are an integral part of geopolitical confrontations. But the question of forming effective mechanisms for countering such digital threats in the aspect of ensuring economic security remains unresolved. This is the approach used in work [6], in which the problem of using information vulnerabilities of the national socio-economic system as a basis for information wars, which became particularly acute with the full-scale invasion of Russia into Ukraine, is actualized. However, the authors of the work do not consider the institutional foundations of strengthening economic security. In continuation of the previous study, the authors of work [7] substantiate the priority of ensuring cyber security under the conditions of hyper securitization and technicalization. However, scientists focus exclusively on technical means for information protection, without considering the broader context of cyber security at the macro level.

Thus, current studies investigate only certain aspects of digitalization of the economy in certain countries and the formation of technical means of information protection; their impact on ensuring the economic security of the state is understudied. Therefore, it is absolutely necessary to improve conceptual approaches to ensure the economic security of the state, taking into account the priority impact of digitalization, given the lack of thorough scientific research on this issue and the strengthening of relevant global threats.

3. The aim and objectives of the study

The purpose of our study is to improve conceptual approaches to ensuring the economic security of the state under the conditions of growing digitalization. This will make it possible to ensure the information security of the national economy, its stability and adaptability to digital risks and threats.

To achieve the goal, the following tasks were set:

– to investigate the current risks and threats to the economic security of the state in the information domain caused by the processes of total digitalization;

– to carry out an assessment of the relationship and interdependence of the level of digital development and the level of cyber security at the macro level;

– to determine the trigger points of the influence of digitalization on the economic security of the state;

– to substantiate the institutional foundations for strengthening the economic security of the state in view of modern security challenges.

4. The study materials and methods

The object of our study is information security of the state and factors that affect the economic security of the state due to vulnerabilities in the information domain. The main hypothesis of the study assumes that the higher the level of digitization of the country, the higher the level of cyber security it should have. Research methodology is based on general scientific and empirical methods of analysis and scientific knowledge, including observation, classification, scientific abstraction, statistical analysis, systematization, and generalization.

In the process of solving the tasks, the method of systematization and generalization was used to study modern risks and threats in the information domain and to form a conceptual scheme of the impact of digitalization on the economic security of the state. Comparative analysis and statistical hypothesis testing (t-test) were used to assess the relationship between the level of digital development (DDL) and the level of cyber security (NCSI) of 154 countries. These initial indicators were calculated by experts from the World Bank [8] and e-Governance Academy [9] based on data from legislative acts, official documents, and official government websites of countries. These include e-Government Development Indicators (EGDI), Network Readiness Indicators (NRI), and countries' readiness to prevent cyber threats and manage cyber incidents. A graphical method was used to analyze the gap between DDL and NCSI. Using the method of correlation-regression analysis, the dependence assessment and modeling of the linear relationship between the cyber security index and the digitization index at the macro level were carried out. With the help of systematization and generalization, conceptual approaches to strengthening the economic security of the state are substantiated in view of modern security challenges, risks, and threats caused by digitalization.

All calculations were carried out using EXSTAT software for statistical analysis and data processing. One-sample t-test function was used to test hypotheses, Pearson Correlation – to measure the strength and direction of the linear relationship between two quantitative variables, and Linear regression – to estimate the linear relationship between dependent and independent variables.

5. Results of research into the key determinants of ensuring the economic security of the state under conditions of digitalization

5. 1. Modern risks and threats to the economic security of the state in the information domain caused by digitalization processes

Modern global trends in the transformation of the national economy are primarily determined by the digitalization of economic relations within the framework of the concept of the information society [10]. World Bank experts note that digitalization of the economy at the global level not only stimulates economic growth but also significantly accelerates its pace, is a driver of innovation, and allows for the creation of new jobs [11]. Together with undeniable advantages and additional opportunities, digitalization is a catalyst for new challenges, risks, and threats [12], which are imperative concepts of security.

The multifaceted nature of the concept of "security" presupposes the multiplicity of its interpretation and application. In the interdisciplinary scientific discourse, security should be considered as a basic characteristic of any socio-economic system, which ensures its stability, integrity, and ability to effectively resist internal and external threats [12]. The highest level in the state security system is national security, which is characterized primarily by the state of the economy, especially in periods of socio-economic instability, economic decline, and crises. At the state level, security is the ability of state institutions to protect sovereignty, ensure stability, and create conditions for the well-being of citizens. Based on the conflict and defense approaches, we maintain the position that the economic security of the state should be considered as the state of the national economy, characterized by stability, economic independence, and the ability for self-development and progress [13].

Under the conditions of total digitalization of the economy, the vector of economic security at all levels of the social hierarchy (individual, society, business, region, state) has changed. A key factor in the development of the national economy on a security basis under the conditions of Industry 4.0 is cyber security, which is considered as the protection of digital data, critical infrastructure, and information systems from cyber threats [2].

As a hierarchical multi-component system, cyber security must be ensured at the macro, meso, and micro levels, taking into account the specificity of the objects of protection, subjects of responsibility, and types of cyber threats. Thus, at the macro level, cyber security involves ensuring the resilience of the socio-economic system to global cyber threats through the formation of a reliable national digital infrastructure and mechanisms for ensuring cyber protection of state information systems, critical infrastructure objects, and state finances [4]. At the meso level, cyber security includes the protection of regional information networks, local authorities, as well as sectors of the economy that are important for regional development, from cyber attacks and technical failures. And at the micro level, cyber security is considered as a process of ensuring data confidentiality, protection against fraud and preservation of operational activities of enterprises, organizations, and individuals [3]. Therefore, there are reasons to assert that ensuring the economic security of the state under the conditions of digitalization requires coordination of efforts at all levels to form a comprehensive system for countering modern digital challenges. Without an appropriate legal framework and an effective institutional environment, digitalization could cause significant damage and create obstacles to the development of the digital economy and ensuring the economic security of the state, regions, enterprises, and individual citizens [13]. In this context, it is also important to develop the skills of mastering modern information and communication technologies [14], to improve the quality of training of specialists, and to stimulate lifelong learning.

Under the conditions of growing turbulence of socio-economic relations, the need of the hour is to monitor the growing number of challenges and threats. At the global level, it has been conducted on a systematic basis for the last two decades by experts from the World Economic Forum to identify and forecast negative security factors. The Global Risk Perception Survey (GRPS) is the main source of original data on global risks and forms the basis of the Global Risks Report 2024 [15]. According to the latest research results, risks in the information domain, namely misinformation and disinformation, are considered the most dangerous global risks in the next two years. This is due to technological changes associated with the rapid development of artificial intelligence technologies, with a simultaneous high level of economic uncertainty and geopolitical tensions. Along with this, cyber attacks and cyber security threats are also among the top five most dangerous risks in the short term. Thus, the exchange of data in real time, the development and use of artificial intelligence and other benefits of digitalization generate global socio-economic risks.

Cybersecurity Ventures estimates that global cybercrime losses exceeded USD 8 trillion in 2023, and this figure is expected to reach USD 10.5 trillion by 2025 [16]. The United States is one of the most affected countries, in which the cost of losses from cyber attacks is about 4 billion dollars per year. European countries are also suffering significant losses due to attacks on business and government infrastructures. In order to minimize these losses, conceptual approaches to ensuring the economic security of the state under conditions of multiple digital risks must be revised.

5. 2. Assessment of the relationship and interdependence of the level of digital development and the level of cyber security at the macro level

Given the vulnerability of countries to cyberattacks, under today's conditions, cyber security and cyber defense play a special role in ensuring the economic security of the national economy [17]. At the global level, cyber security is assessed using a number of indices that include the readiness of countries to prevent cyber threats and manage cyber incidents, the most significant of which are the National Cyber Security Index (NCSI), the Global Cybersecurity Index (GCI), and the Cybersecurity Exposure Index (CEI). The values of these indices for individual countries are given in Table 1.

In 2024, countries with the highest levels of cybersecurity include Finland, Norway, and Denmark, which performed best with effective defense infrastructure and proactive cyber-

security measures. Finland tops the global rankings with an overall cybersecurity index of 92.81, while Norway and Denmark also have similarly high security scores. Other countries with high levels of cyber security include Australia, the UK, and Sweden, which continue to invest in cyber security [19].

The growing number of fundamentally new threats associated with the rapid digital development of most countries of the world dictates the objective necessity of forming a security-oriented information environment and reliable information protection systems as the most important asset today. Therefore, it is possible to put forward a hypothesis that the higher the level of digitalization of a country, the higher the level of cyber security it should have. To test this hypothesis, we shall use a set of statistical research methods.

At the first stage, we shall conduct a comparative analysis of the level of digital development and the level of cyber security of countries (Table 2) in 2023 using the National Cyber Security Index calculated by the e-Governance Academy [9].

Table 1

The level of cyber security of countries

No.	Country	National Cyber Security Index	Cybersecurity Exposure Index	Global Cybersecurity Index	Cyber Resilience Index	Final Cyber Safety Score
1	Finland	85.71	89	95.78	93.64	92.81
2	Norway	67.53	86.6	96.89	94.39	92.63
3	Denmark	84.42	88.3	92.6	96.44	92.45
4	Australia	66.23	86.9	97.47	85.61	89.99
5	Great Britain	89.61	79.3	99.54	90.40	89.75
6	Sweden	84.42	79	94.55	95.10	89.55
7	Austria	85.71	83.8	93.89	90.95	89.55
8	Japan	63.64	86.2	97.82	82.29	88.77
9	USA	64.94	85.5	100	80.31	88.60
10	Canada	70.13	79.3	97.67	88.01	88.33

Source: compiled by Authors based on data from [18].

Table 2

Comparative analysis of digital development level (DDL) and cyber security index (NCSI) of countries

Country	DDL	NCSI	GAP (NCSI–DDL)	Country	DDL	NCSI	GAP (NCSI–DDL)
Switzerland	82.93	75.32	–7.61	Portugal	68.46	89.61	21.15
Denmark	82.68	84.42	1.74	Lithuania	67.34	93.51	26.17
Korea	68.83	82.23	–13.4	Italy	67.26	79.22	11.96
Netherlands	81.86	83.12	1.26	Latvia	66.23	75.32	9.09
Sweden	81.51	84.42	2.91	Slovakia	65.44	83.12	17.68
USA	81.05	64.94	–16.11	Russian Federation	65.12	71.43	6.31
Norway	80.19	67.53	–12.66	Poland	65.03	87.01	21.98
Germany	80.01	90.91	10.9	Croatia	64.63	83.12	18.49
Great Britain	79.96	89.61	9.65	Hungary	64.25	67.53	3.28
Singapore	79.93	71.43	–8.5	Greece	64.02	89.61	25.59
Japan	78.69	63.64	–15.05	Saudi Arabia	63.89	84.42	20.53
Iceland	78.64	55.84	–22.8	China	62.41	51.95	–10.46
Luxembourg	78.4	66.23	–12.17	Belarus	62.33	53.25	–9.08
Finland	78.35	85.71	7.36	Malaysia	62.19	79.22	17.03
Australia	77.61	66.23	–11.38	Bulgaria	62.06	74.03	11.97
France	77.29	84.42	7.13	Kazakhstan	60.18	48.05	–12.13
New Zealand	76.81	51.95	–24.86	Romania	59.84	89.61	29.77
Canada	75.96	70.13	–5.83	Serbia	59.81	80.52	20.71
Austria	75.76	85.71	9.95	Turkey	58.29	61.04	2.75
Estonia	75.59	93.51	17.92	Moldova	56.79	57.14	0.35
Israel	75.5	67.53	–7.97	Ukraine	55.96	75.32	19.36
Ireland	75.18	75.32	0.14	Azerbaijan	63.64	54.78	8.86
Belgium	74.07	94.81	20.74	Georgia	53.5	64.94	11.44
Spain	72.21	88.31	16.1	Egypt	46.93	57.14	10.21
Malta	71.74	50.65	–21.09	Libya	41.1	10.39	–30.71
Czech Republic	69.21	90.91	21.7	India	40.02	67.53	27.51
UAE	68.87	40.26	–28.61	Nepal	30.58	28.57	–2.01
	– the level of cyber security is higher than the level of digital development				– the level of cyber security is lower than the level of digital development		

Source: compiled by Authors according to the e-Governance Academy [9].

The top ten according to NCSI include European countries, the USA, and Canada. Ukraine has the fastest growth rate of NCSI, which as of 04/30/2024 according to this indicator, it rose to 11th place among all countries of the world. According to the results of the comparison, it was found that a significant number of countries with a high level of digital development have an insufficient level of cyber security, such as New Zealand, the USA, Japan, and Norway. On the other hand, in Lithuania, Belgium, the Czech Republic, Romania, Portugal, Poland, and Ukraine, the level of cyber security is growing even faster than the level of penetration of digital technologies. To check whether the average value of the sample (the level of cyber security for countries with a high level of digitalization) is significantly different from the given or expected average value, we use the one-sample *t*-test. The null hypothesis (H_0) is accepted, according to which the average level of cyber security for countries with a high level of digitalization is equal to the average for all countries. The alternative hypothesis (H_1) implied that the average level of cyber security for countries with a high level of digitalization is higher than the average value.

After performing the *t*-test using EXSTAT, our results are given in Table 3.

Since the obtained *p*-value<0.05, it could be concluded that the level of cyber security in highly digitized countries is statistically significantly different and higher than the overall average. The hypothesis was confirmed, so the gap between the Digital Development Level and the National Cyber Security Index was analyzed at the next stage. For this purpose, the graphic method was used shown in Fig. 1, where the countries are ranked from left to right as the amount of digitization decreases.

Table 3

T-test of the hypothesis that countries with a high level of digitalization should have a higher level of cyber security

Indicator	Number of countries under observation	Minimum value	Maximum value	Average value	Standard deviation
NCSI	154	3.900	94.810	46.450	26.137
DDL	154	11.300	82.680	51.006	18.242
Hypothesis *T*-test results for NCSI					
Normality test:		One-sample t-test/Two-tailed test (NCSI):			
Shapiro-Wilk test (NCSI):		*t* (Observed value)		22,054	
W	0,950	|*t*| (Critical value)		1.976	
p-value (Two-tailed)	<0,0001	*p*-value (Two-tailed)		<0.0001	
alpha	0,05	alpha		0.05	
Hypothesis *T*-test results for DDL					
Normality test:		One-sample t-test/Two-tailed test (DDL):			
Shapiro-Wilk test (DDL):		*t* (Observed value)		34,698	
W	0,970	|*t*| (Critical value)		1.976	
p-value (Two-tailed)	0,002	*p*-value (Two-tailed)		<0.0001	
alpha	0,05	alpha		0.05	

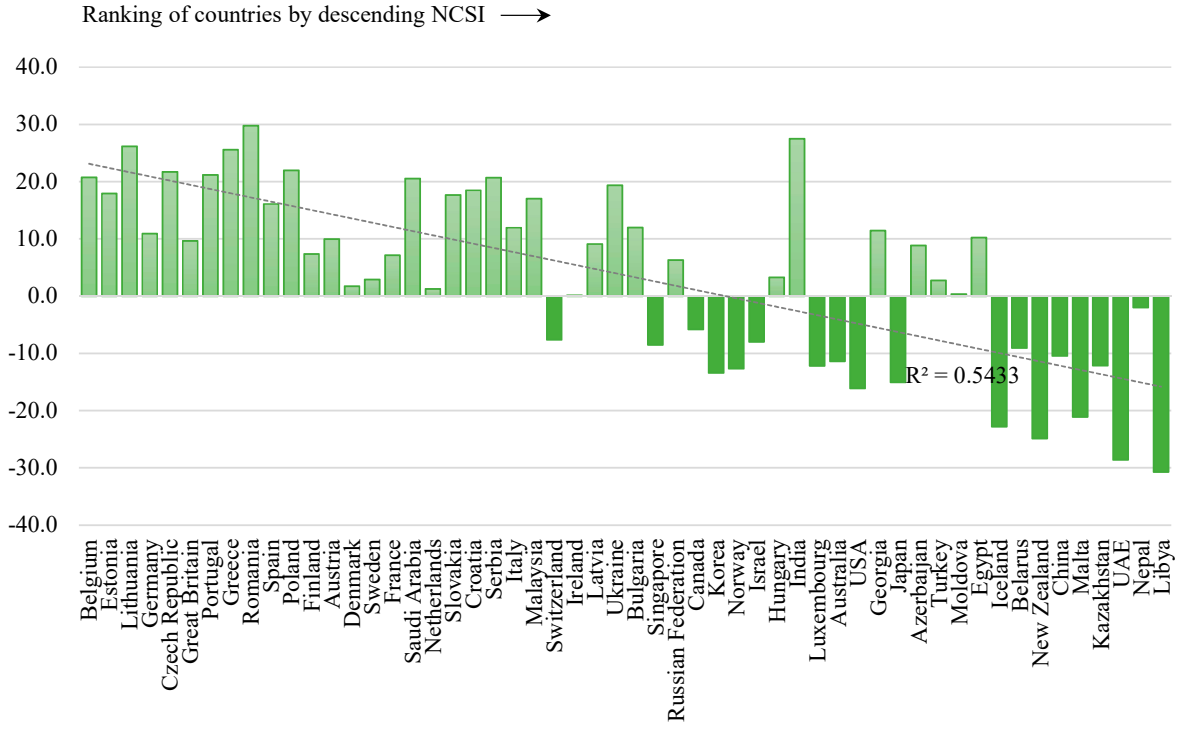

Fig. 1. Analysis of the gap between the level of digitalization and the level of cyber security of countries

Using the graphic method, the uneven development of cyber security and digitalization in the vast majority of countries was revealed. Thus, in countries with a high level of the National Cyber Security Index, its value significantly exceeds the level of digitization. Whereas in countries with a lower level of cyber security, the digital society is more developed than the national domain of cyber security.

High levels of cyber security in countries with lower digital penetration may indicate a conscious investment in cyber security to keep data and digital infrastructure secure and policies in place to prevent cyber threats at an early stage. That is, these countries choose a proactive strategy, seeking to protect even relatively low levels of the digital economy. Ukraine belongs to this group of countries. Undoubtedly, this policy is strategically justified under the conditions of the information war unleashed by Russia against Ukraine and the increased level of cyber risks. Investing in security in advance and forming a security-oriented information environment for the digital economy at the stage of its formation is the basis of a proactive approach to ensuring the economic security of the state. According to it, even the initial small volume of the digital economy should be well protected to avoid large losses in the future. Countries that choose this approach may be more prepared to expand their digital infrastructure in the future, as having strong cybersecurity mechanisms allows new digital technologies to be adopted with less risk.

Instead, countries with a low level of cyber security but high digitalization are characterized by a focus on the rapid development of digital technologies without due attention to their protection, which increases the risk of cyber threats. Such countries pay more attention to the implementation of digital technologies, leaving the issue of cyber security secondary. However, a lack of adequate investment in cybersecurity could lead to vulnerabilities in key areas such as financial systems, government institutions, and private user data. In general, a high level of digital technology means a greater number of vulnerabilities that could be exploited by cybercriminals [20], thus creating potential challenges for the stable functioning of digital infrastructure, especially in the event of serious cyber attacks.

A schematic representation of data on the cyber power of countries and their chosen policy of ensuring economic security in the digital age is shown in Fig. 2.

Most countries are expanding digital services and the size of the digital economy but not all of them have a high level of cyber security [21]. This is often explained by the fact that many of these countries are committed to improving their cyber security, but have a significant deficit in cyber capabilities, limited resources, personnel, access to equipment and stable funding [22]. However, it is worth noting that countries that prioritize the initial development of digital technologies over the integration of cybersecurity risk a more dangerous and less resilient cyberspace.

Comparing the NGSI indicators with the general development of information and communication technologies, it should be noted that certain countries, realizing the importance of cyber risks, are actively engaged in cyber security, while having a relatively low rate of digitalization. This means they are well positioned to create a safe and secure cyberspace.

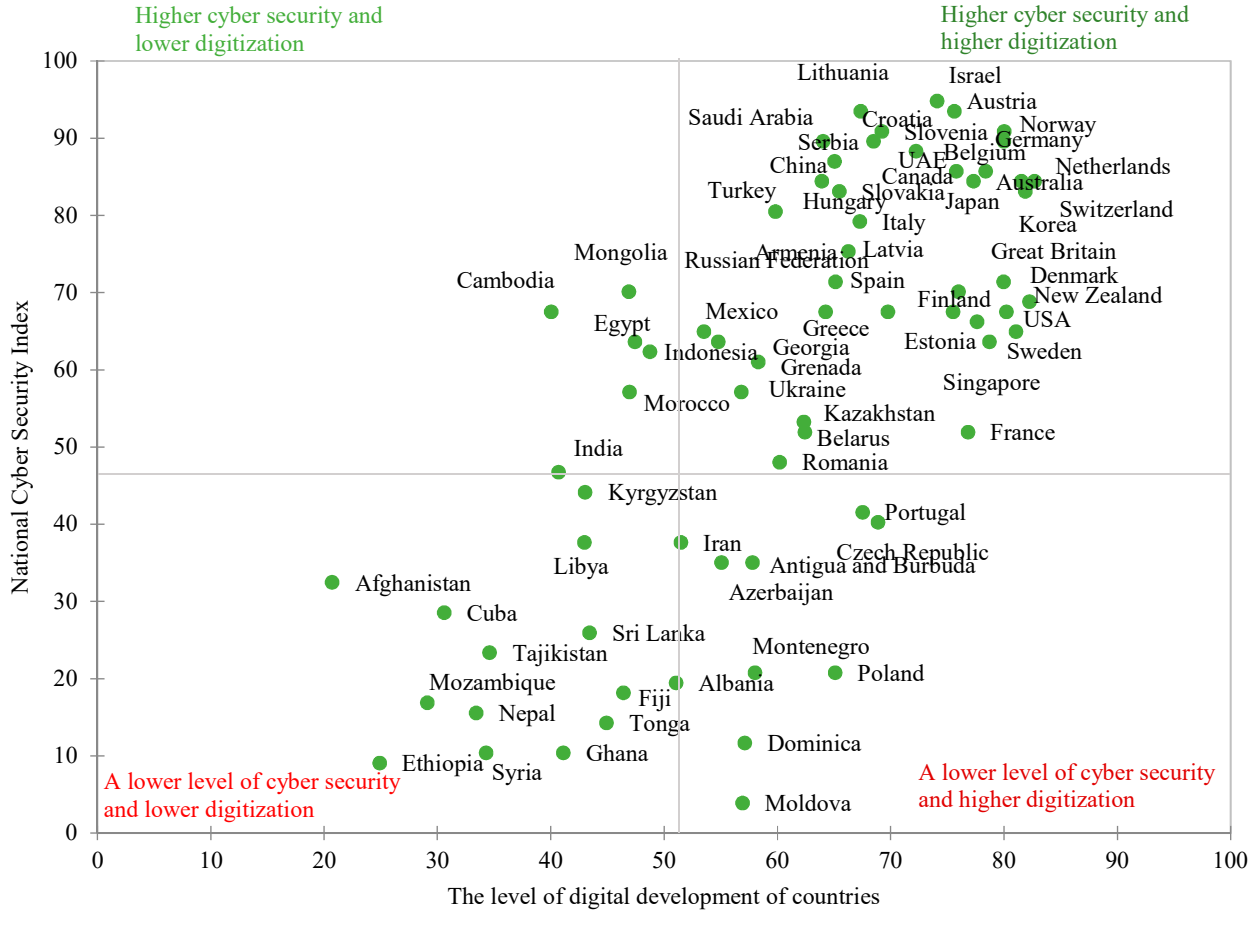

Fig. 2. The level of digital development of countries compared to the National Cyber Security Index in 2023

It is preliminarily determined that the level of cyber security in countries with high digitization is statistically significantly different and higher than the overall average. Therefore, it is advisable to analyze in more detail the relationship and interdependence of the level of digital development and the level of cyber security using the correlation-regression analysis method.

For this purpose, the Pearson correlation coefficient (r) (1) was used:

$$r(DDL;NCSI) = \frac{n\sum DDL \cdot NCSI - \sum DDL \sum NCSI}{\sqrt{\left(n\sum DDL^2 - \left(\sum DDL\right)^2\right)\cdot\left(n\sum NCSI^2 - \left(\sum NCSI\right)^2\right)}}, \quad (1)$$

where *DDL* is Digital Development Level; *NCSI* – National Cyber Security Index; n is the number of pairs of values (sample).

Based on the results of calculations using the EXSTAT software, it was determined that r (DDL; NCSI)=0.701, which indicates a moderately strong positive linear relationship between the level of digital development and cyber security. This means that as countries accelerate their digital transformation, their level of cyber security tends to increase as well. The identified relationship between digitization and cyber security is statistically significant at a high level of confidence and is not the result of random fluctuations, as indicated by the obtained p-values (Pearson)<0.0001. In other words, there is a very low probability (less than 0.01 %) that such a connection occurred by chance.

The value of the calculated Coefficients of determination (Pearson) R^2=0.491 means that approximately 49.1 % of the variation in the level of cyber security of countries could be explained by the variation in the level of digital development. This is quite a high indicator for socio-economic data, which indicates that digitalization is a significant factor influencing cyber security. Among other factors that determine the remaining 50.9 % of the variation, it is possible to highlight the features of the state security regulation policy, investments in cyber protection, the level of education in the field of cyber security, legislative initiatives, etc.

To model the linear relationship between digitalization and cyber security indices, a regression analysis was conducted using EXSTAT software. The results are given in Table 4 and Fig. 3.

Regression analysis reveals a strong positive relationship between the level of digitization and cyber security. Countries with higher levels of digital technology tend to better protect their infrastructure, although there are other factors that could also affect cybersecurity. On average, with an increase in the digitization index by 1 unit, the cyber security index increases by 0.70 units. At the same time, the level of digitization is the main factor affecting cyber security.

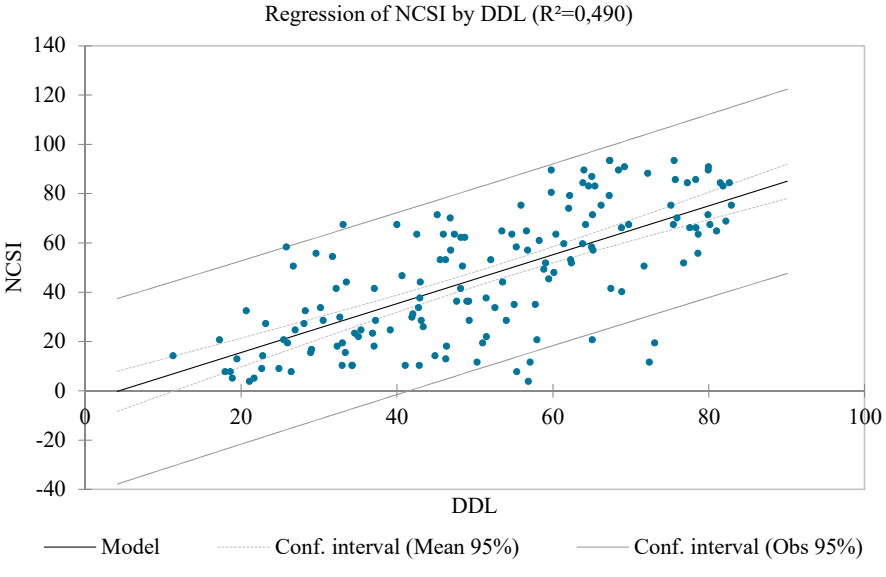

Fig. 3. Modeling the linear relationship between the level of digitalization and the level of cyber security of countries in 2023

Table 4

Results of the regression analysis between the level of digitalization (DDL) and the level of cyber security

Stage	Regression analysis parameters							
Analysis of Variance	Source	DF	Sum of squares	Mean squares	*F*	*Pr>F*	Designation codes *p*-values	
	Model	1.000	50,485.016	50,485.016	146.078	<0.0001	***	
	Error	152.000	52,531.717	345.603	–	–	–	
	Corrected amount	153.000	103,016.73	–	–	–	–	
	Calculated from the model *Y*=Mean(*Y*); Designation codes: 0<***<0.001<**<0.01<*<0.05<.<0.1<°<1							
Model parameters	Source	Value	Standard Error	*t*	*Pr>|t|*	Lower limit (95 %)	Upper limit (95 %)	Designation codes *p*-values
	Intercept	–4.283	4.447	–0.963	0.337	–13.069	4.503	°
	DDL	0.991	0.082	12.086	<0.0001	0.829	1.153	***
	Designation codes: 0<***<0.001<**<0.01<*<0.05<.<0.1<°<1							
	Model equations: 94.81=–4.28342977727939+0.991061274368306*74.07							
Standardized coefficients	Source	Value	Standard Error	*t*	*Pr>|t|*	Lower limit (95 %)	Upper limit (95 %)	Designation codes *p*-values
	DDL	0.700	0.058	12.086	<0.0001	0.586	0.814	***
	Designation codes: 0<***<0.001<**<0.01<*<0.05<.<0.1<°<1							

5. 3. Determining trigger points of influence of digitalization on the economic security of the state

Our research and generalization of the features of the manifestation of destructive factors of economic security in the information domain [3, 11–13, 15, 23] make it possible to determine the trigger points of the influence of information security on the economic in the countries of the world. These include economic losses as a result of cyberattacks on the critical infrastructure of the national economy, financial losses due to leakage of data and confidential information, as well as losses from cybercrime.

The biggest economic losses could be caused by cyber-attacks on energy systems, transport, or financial networks. An example is the attack on the Ukrainian energy system during the Russian Federation's large-scale invasion of Ukraine, which affected the supply of electricity to millions of people and caused significant damage to the economy. As for financial losses due to data leaks, they could cost companies hundreds of millions of dollars, through fines, compensation to customers, and security enhancement costs [23].

Cybercrime losses suffered by financial institutions and public authorities due to fraud, identity theft, and cyber-attacks could disrupt normal business processes and hinder or make impossible the activities of public and commercial enterprises, institutions, and institutions. For example, attacks using special programs (ransomware) have become a serious problem for business in the world, especially in the USA and European countries, causing billions of dollars in damage to companies every year.

Considering the genesis of destructive security factors, digitalization risks could have a low, medium, or high probability of adverse events. Based on the results of systematization and generalization, it is possible to build a conceptual diagram of the impact of digitalization risks on the economic security of the state (Fig. 4).

The level of risk depends on its nature; however, it may not be realized at all depending on the conditions of the information environment of the national economic system. In the information environment, mechanisms should be formed to prevent the transformation of risk into a threat. In the opposite case, in case of an insufficient level of cyber protection, risks turn into threats. Among the most dangerous threats of digitalization worth highlighting are leakage, violation of integrity, blocking of information, damage to critical infrastructure objects using digital technologies, as well as interference with the activities of state and commercial enterprises, institutions, and organizations [24]. The consequences of their implementation could be acceptable, critical, or catastrophic in case of ineffectiveness or inefficiency of the system of ensuring the economic security of the state.

In the existing approach to the management and detection of threats to the economic security of Ukraine, their classification is used only according to the criterion of source into internal and external. At a time when a broader scientific discourse exposes threats to the economic security of the state to a broader classification: by directions of influence on financial activity, degree of danger, possibility, and scope of action, by its duration, nature of influence, etc. This indicates that Ukrainian laws and reforms are lagging behind international scientific opinion in the field of economic security, which significantly complicates the process of identifying threats to the economic security of Ukraine, prevents them from building a clear hierarchy and passporting threats. The latter is the basis for the formation of preventive measures to prevent the transformation of existing risks into threats that destabilize the activities of state institutions and businesses.

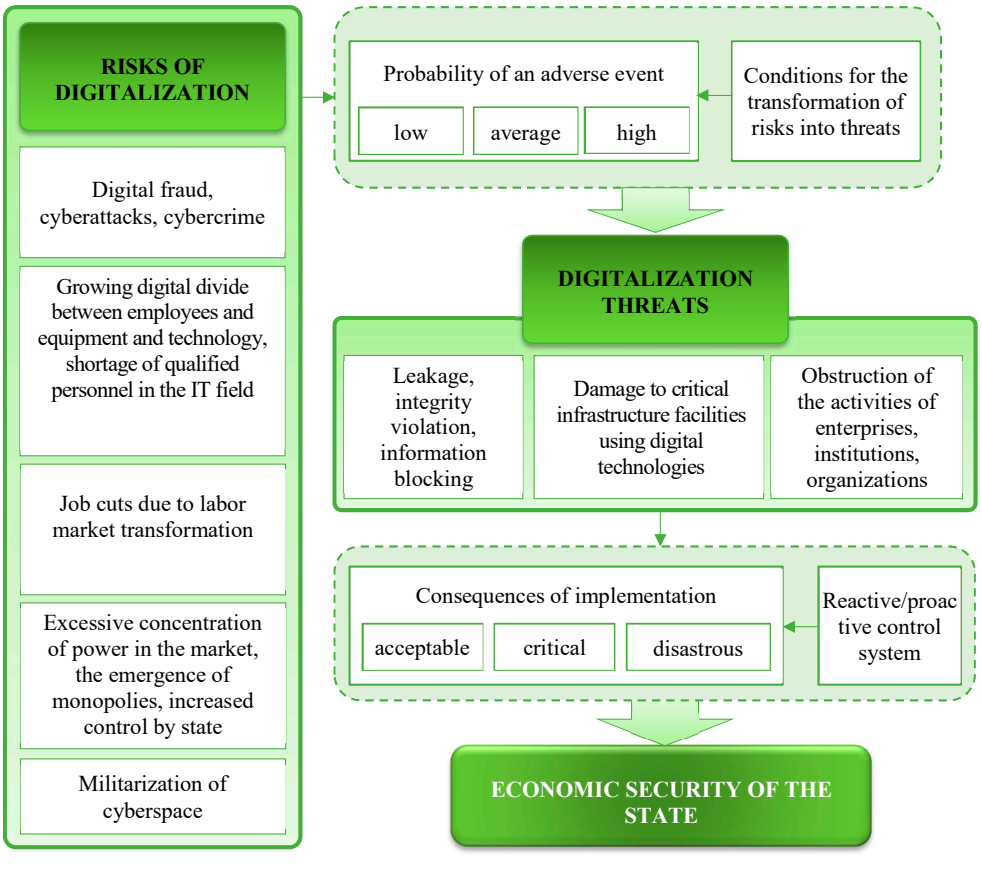

Fig. 4. Conceptual diagram of the influence of digitalization on the economic security of the state

5. 4. Substantiation of the institutional foundations for strengthening the economic security of the state in view of modern security challenges

State management of processes for preventing risks and threats to economic security in the information domain is based on a number of tools [25] used in different countries to protect against cyber threats. The vast majority of them are based on special legislation and regulatory acts on the regulation of cyberspace. For example, the General Data Protection Regulation (GDPR) in the EU [26] establishes strict rules for the protection of personal data, and in the USA, there are laws on the protection of critical infrastructure, which are aimed at protecting energy, transport, and financial systems from cyber attacks. The vast majority of countries with high cyber security index values implement national cyber security strategies to coordinate the actions of public and private entities. For example, the UK Cyber Security Strategy 2022–2030 [27] defines the priorities of the state in the protection of the information space and includes a comprehensive system of prevention and response to cyber attacks.

From an institutional point of view, ensuring the economic security of the state in the face of multiple digital risks and threats in most countries of the world with a high level of the cyber security index occurs through the functioning of specialized cyber security agencies. They monitor and prevent cyber threats. Examples include the US Cybersecurity and Infrastructure Security Agency (CISA) [28] and the EU Cybersecurity Agency (ENISA) [29] which provide guidelines, standards, and respond to cyber attacks.

Taking into account the international experience under the conditions of multiple digital risks, the need of the hour is the implementation of a two-stage proactive approach to ensuring the economic security of the state. At the first stage, a security-oriented information environment should be formed to prevent the transformation of cyber risks into threats. At the second stage, an effective system of ensuring economic security at all levels of the social hierarchy (state, business, individual, society) should be created, aimed at preventing the realization of the threat or minimizing its consequences.

Organizationally, to ensure information and economic security, cooperation between the state and private companies is important [30, 31], which makes it possible to exchange information and jointly respond to cyber threats [32]. For example, in the USA there are programs like InfraGard, which unite the government and the private sector to jointly protect the infrastructure [33]. In addition, countries around the world are investing in improving the skills of cyber security specialists through educational programs and trainings. Initiatives such as CyberCorps [34] in the US provide training for new personnel to protect public and private networks from cyber threats.

The above tools help the governments of the countries of the world to effectively face risks and threats to the economic security of the state in the field of information security, creating integrated protection systems at the national level. In the absence of proactive provision of economic security, digitalization risks are transformed into challenges and threats to the economic security of the state. The most dangerous of them are a decrease in the competitiveness of the national economy due to the loss of prospects for innovative development, an insufficient level of personnel support for accelerated economic growth based on digitization. It is also possible to have institutional deformations with the emergence of new business processes, such as corruption in government bodies at both the macro and meso levels, and others.

6. Discussion of results based on improving conceptual approaches to ensuring economic security under the conditions of digitalization

Our research results confirm the need for a two-stage implementation of a proactive approach to ensuring the economic security of the state through the formation of a security-oriented information environment and counteracting negative security factors at all levels of the social hierarchy. This is explained by the growing impact of digital risks and threats according to the Global Risk Perception Survey (GRPS) [15] and Cybersecurity Ventures estimates [16], confirmed in the course of the study by the close connection and interdependence between the level of digitalization and the level of cyber security (Tables 3, 4, Fig. 1–3), as well as identified trigger points of the impact of digitalization on the economic security of the state based on [11, 15, 23].

The need for comprehensive monitoring of digital threats to the economic security of the state is justified because digital transformation has currently covered all domains of socio-economic relations. This significantly distinguishes our results from [10], in which attention is focused on the advantages and additional opportunities from the implementation of digital technologies, and from [13, 14], in which individual digital risks and threats are analyzed. This becomes possible thanks to the analysis of digital transformation processes and the level of cyber security at the national level for a significant number of countries, in contrast [21] and using previous research results [4]. The identification of the trigger points of the influence of digitalization on the economic security of the state, in contrast to [3], largely solves the problem of forming digital economy strategies in accordance with modern security requirements.

The introduction of a fundamentally new approach to ensuring the economic security of the state in view of modern security challenges makes it possible to increase the national stability of countries under the conditions of the digital transition. This is an advantage of this study in comparison with similar known ones [6, 20, 24] and it makes it possible to apply a broader context of cyber security at the macro level, which goes beyond the scope of exclusively technical means of protection.

Delays in providing data on the level of digital development of different countries, as well as the lack of a single methodology for assessing the level of economic security of the state for all countries, are significant limiting factors for conducting research. This makes it much more difficult to identify the trigger points of digitalization risks. Therefore, the main drawback of the study is the impossibility of comparing the level of digitalization and cyber security with the level of economic security of the state. It is in this direction that further research could be developed to devise a unified methodology for assessing economic security for different countries of the world.

Prospects for further research on the outlined issues relate to analysis of factors that affect the level of cyber security as determinants of the economic security of the state. Worth investigating is the level of investments in cyber security, legislative regulation, training programs on cyber security, challenges related to the rapid development of artificial intelligence and its integration into all domains of the economy. It is also important to carry out scientific substantiation of mechanisms for increasing national resilience to digital risks and threats.

7. Conclusions

1. The increasing level of digitization of the economy makes it vulnerable to digital risks and threats. The paradigm and theory of economic and information security, which worked well in a relatively stable world, cannot be combined with new, unpredictable global threats. The formation of a security-oriented information environment is an important prerequisite for maintaining the stability of the functioning of the national economy, reducing social tension in society under conditions of uncertainty, ensuring economic growth and the well-being of the population.

2. It has been proven that the level of digitalization and cyber security have a close linear relationship: countries with more developed digital technologies usually demonstrate a higher level of cyber security. The more a country's digital infrastructure develops, the more attention is paid to data protection and cyber security. Digital development is one of the key factors influencing the level of cyber security and economic security under the conditions of Industry 4.0. Countries with high levels of cyber security but relatively low digitization may have better prospects and potential for further digital development with fewer risks. These countries could safely implement new digital tools by having robust safeguards in place. On the other hand, countries with high digitalization and low levels of cyber security may experience greater losses from cyber threats, and insufficient information security may slow down the pace of digital progress due to potential threats arising from unprotected infrastructure. Ideally, countries should strive for a balance between the level of digitization and the level of cybersecurity to ensure the safe and sustainable development of the digital economy.

3. The identified trigger points of the impact of information security on the economy indicate that cyber security issues could have a significant impact on the economy of any country. They could cause not only direct financial losses but also a loss of trust in international institutions and a decrease in the investment attractiveness of national economies. Thus, in the context of ensuring the economic security of the state under the conditions of total digitalization, information security is the need of the hour. However, as evidenced by our research results, quite often insufficient attention is paid to the formation of a security-oriented information environment at the macro level. Focusing efforts only on countering threats that have already materialized, leaving certain digital risks outside the existing stabilization policy and economic reforms, does not make it possible to ensure the stability of the national economy under conditions of digitalization. That is why new research indicates the critical obsolescence of traditional approach to both solving problems and identifying them.

4. To ensure economic security within Industry 5.0, it is necessary to form a security-oriented information environment of the national economy, to make significant investments in data protection, and to form institutional mechanisms for its provision, taking into account the challenges of digitalization. Effective countermeasures against threats to the economic security of the state and risk control depend on a national monitoring system capable of timely responding to changes and reflecting the real situation in the system. Updating and expanding the normative-methodical approach, as well as ensuring the dynamic development of analytical capacities, are priorities in the system for ensuring the economic security of the state under the conditions of digitalization.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Funding

The research was carried out within the framework of the state budget topic "Formation of a security-oriented information environment to increase the economic security of Ukraine in the war and post-war periods" state registration number: 0124U000615.

Data availability

The manuscript has associated data in the data warehouse.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

References

1. Heath, B. J. (2020). The new national security challenge to the economic order. The Yale Law Journal, 129 (4), 1020–1098. Available at: https://www.yalelawjournal.org/pdf/HeathArticle_jx8mdn4b.pdf
2. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. Economic and Cyber Security, 30–58. https://doi.org/10.15587/978-617-7319-98-5.ch2
3. Anand, S. C., Teixeira, A. M. H., Ahlén, A. (2024). Risk Assessment of Stealthy Attacks on Uncertain Control Systems. IEEE Transactions on Automatic Control, 69 (5), 3214–3221. https://doi.org/10.1109/tac.2023.3318194
4. Yusif, S., Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. Journal of Applied Security Research, 16 (4), 490–513. https://doi.org/10.1080/19361610.2021.1918995
5. Edelman, R. D. (2024). Rethinking Cyber Warfare. Oxford University Press. https://doi.org/10.1093/9780197509715.001.0001
6. Lysenko, S., Marukhovskyi, O., Krap, A., Illiuschenko, S., Pochapska, O. (2023). The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War. Studies in Media and Communication, 11 (7), 150. https://doi.org/10.11114/smc.v11i7.6414
7. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4 (1). https://doi.org/10.1093/cybsec/tyy006

8. Global Cyber Security Index. European Union.
9. National Cyber Security Index. E-Governance Academy. Available at: https://ncsi.ega.ee/ncsi-index/
10. Teece, D. J. (2018). Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world. Research Policy, 47 (8), 1367–1387. https://doi.org/10.1016/j.respol.2017.01.015
11. Digital Progress and Trends Report 2023 (2024). World Bank. https://doi.org/10.1596/978-1-4648-2049-6
12. Onyshchenko, V., Yehorycheva, S., Maslii, O., Yurkiv, N. (2021). Impact of Innovation and Digital Technologies on the Financial Security of the State. Proceedings of the 3rd International Conference on Building Innovations, 749–759. https://doi.org/10.1007/978-3-030-85043-2_69
13. Onyshchenko, V., Onyshchenko, S., Maslii, O., Maksymenko, A. (2023). Systematization of Threats to Financial Security of Individual, Society, Business and the State in Terms of the Pandemic. Proceedings of the 4th International Conference on Building Innovations, 749–760. https://doi.org/10.1007/978-3-031-17385-1_63
14. Bencsik, A. (2020). Challenges of Management in the Digital Economy. International Journal of Technology, 11 (6), 1275. https://doi.org/10.14716/ijtech.v11i6.4461
15. Global Risks Report 2024. World Economic Forum. Available at: https://www.weforum.org/publications/global-risks-report-2024/
16. Dovhan, O. (Ed.) (2023). Kiberbezpeka vinformatsiynomu suspilstvi. Informatsiyno-analitychnyi daidzhest. Kyiv. Available at: https://ippi.org.ua/sites/default/files/2023-7.pdf
17. Onyshchenko, S. V., Masliy, O. A., Buriak, A. A. (2023). Threats and Risks of Ecological and Economic Security of Ukraine in the Conditions of War. 17th International Conference Monitoring of Geological Processes and Ecological Condition of the Environment, 1–5. https://doi.org/10.3997/2214-4609.2023520072
18. Lynn, S. (2024). Countries With The Highest Cyber Threat Risk And Ones With The Lowest: Report. Available at: https://www.mescomputing.com/news/4208968/countries-cyber-threat-risk-ones-lowest-report
19. Global cybersecurity ranking 2024: Which countries are most at risk? (2024). SecurityDive. Available at: https://securitydive.in/2024/05/14/global-cybersecurity-ranking-2024-which-countries-are-most-at-risk/
20. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Cherviak, A. (2023). Cybersecurity and improvement of the information security system. Journal of the Balkan Tribological Association, 29 (5), 818–835.
21. Rong, K. (2022). Research agenda for the digital economy. Journal of Digital Economy, 1 (1), 20–31. https://doi.org/10.1016/j.jdec.2022.08.004
22. Onyshchenko, S., Maslii, O., Kivshyk, O., Cherviak, A. (2023). The impact of the insurance market on the financial security of Ukraine. Financial and Credit Activity Problems of Theory and Practice, 1 (48), 268–281. https://doi.org/10.55643/fcaptp.1.48.2023.3976
23. Financial watchdog fines Equifax Ltd £11 million for role in one of the largest cyber security breaches in history. Financial Conduct Authority. Available at: https://www.fca.org.uk/news/press-releases/equifax-ltd-fine-cyber-security-breach
24. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V. (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations, 791–803. https://doi.org/10.1007/978-3-031-17385-1_67
25. Krasnobayev, V., Yanko, A., Hlushko, A. (2023). Information Security of the National Economy Based on an Effective Data Control Method. Journal of International Commerce, Economics and Policy, 14 (03). https://doi.org/10.1142/s1793993323500217
26. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Official Journal of the European Union, L119. Available at: http://data.europa.eu/eli/reg/2016/679/oj
27. HM Government. Government Cyber Security Strategy: 2022 to 2030. Available at: https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/government-cyber-security-strategy-2022-to-2030-html
28. Cybersecurity and Infrastructure Security Agency (CISA). U.S. Department of Homeland Security.
29. The European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/
30. Onishchenko, S., Matkovskyi, A., Puhach, O. (2014). Analysis of threats to economic security of Ukraine in conditions of innovative economic development. Economic Annals-XXI, 1-2 (2), 8–11. Available at: https://ea21journal.world/index.php/ea-v138-02/
31. Onyshchenko, S., Yehorycheva, S., Furmanchuk, O., Maslii, O. (2020). Ukraine Construction Complex Innovation-Oriented Development Management. Proceedings of the 2nd International Conference on Building Innovations, 687–700. https://doi.org/10.1007/978-3-030-42939-3_68
32. Svistun, L., Glushko, A., Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. International Journal of Engineering & Technology, 7 (3.2), 447. https://doi.org/10.14419/ijet.v7i3.2.14569
33. InfraGard. Available at: https://www.infragard.org/
34. CyberCorps. Available at: https://www.cybercorps.org/