This study's object is the process that provides for the state's economic security in the context of digital transformation, which is accompanied by the growth of cyber threats and digital risks. Its relevance is predetermined by the urgent need to rethink approaches to cybersecurity and the growing dependence of the economy on information technologies. The issue is the insufficient integration of security-oriented mechanisms into national digital development strategies, which limits the state's ability to counter hybrid threats and ensure the resilience of critical infrastructures.

This study confirms the presence of a statistically significant inverse relationship between the level of information and communication technologies development and cybersecurity (correlation coefficient $r = -0.763$, $p < 0.05$), indicating a potential technological imbalance. A concept of digital risk mitigation has been proposed, which integrates generative artificial intelligence (GAI) into the analytical, infrastructural, regulatory, and educational components of the national cybersecurity system.

The proposed approach is based on the application of regression modeling, comparative analysis of international indices, graph-analytical visualization, and expert evaluation, providing interdisciplinary coverage of the research domain. It has been shown that the effectiveness of intelligent security solutions depends significantly on institutional maturity, transparency of the regulatory environment, access to data, digital inclusion, and readiness for cross-sectoral cooperation.

The findings can be applied to enhance national digital policy and design a strategic framework for integrating GAI into the state's economic security system, particularly under wartime conditions

Keywords: economic security, generative artificial intelligence, cybersecurity, security-oriented information environment

UDC 338.246-049.5:004.89
DOI: 10.15587/1729-4061.2025.336640

MINIMIZATION OF DIGITAL RISKS AND THREATS TO THE ECONOMIC SECURITY OF THE STATE THROUGH THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE

Alona Buriak
Corresponding author
PhD, Associate Professor
Department of International Economic Relations and Tourism*
E-mail: a_buriak@ukr.net
Oleksandra Maslii
PhD, Associate Professor
Department of Finance, Banking and Taxation*
*National University «Yuri Kondratyuk Poltava Polytechnic»
Vitaliya Hrytsayenka ave., 24, Poltava, Ukraine, 36011

Received 01.05.2025
Received in revised form 16.06.2025
Accepted 09.07.2025
Published 23.07.2025

How to Cite: *Buriak, A., Maslii, O. (2025). Minimization of digital risks and threats to the economic security of the state through the use of generative artificial intelligence. Eastern-European Journal of Enterprise Technologies, 4 (13 (136)), 17–25. https://doi.org/10.15587/1729-4061.2025.336640*

1. Introduction

The current stage of development of the digital economy is accompanied by a rapid increase in risks and threats that affect the stability of the functioning of state institutions, businesses, and society as a whole. This problem is particularly relevant for Ukraine, which, under the conditions of a full-scale war, is facing multi-level challenges in the field of cybersecurity, protection of critical digital infrastructure, and ensuring economic stability. Digital transformation, on the one hand, opens up new opportunities for the modernization of management processes, the development of electronic services, strengthening the institutional environment, and on the other hand, forms a new configuration of vulnerabilities that require a systemic state response. Under modern conditions of globalization and digital transformation, state economic systems are faced with new challenges, in particular, digital risks and cyber threats that can seriously affect the economic security of states. In-depth study of these issues is relevant because digital technologies, although they open up new opportunities for economic development, at the same time create numerous threats that require comprehensive analysis and development of mechanisms for their neutralization.

The impact of digital technologies on economic security is not unambiguous: a high level of development of information and communication technologies (ICT) does not guarantee an adequate level of cyber protection. An analysis of the comparative dynamics of ICT and the cybersecurity index in 25 countries revealed the presence of a feedback loop between the speed of digitalization and the effectiveness of measures to counter cyber threats. This indicates insufficient integration of security components into the digital development strategy, which highlights the need to form a security-oriented information environment.

At the same time, generative artificial intelligence opens up new horizons in the field of countering digital threats. Its ability to detect anomalies, adaptive learning and highly accurate threat identification creates the potential to transform approaches to ensuring economic security. The integration of AI into the digital architecture of public administration, critical infrastructure, and corporate systems can significantly

increase the level of cyber resilience and reduce vulnerability to hybrid attacks. The practical implementation of such intelligent systems will make it possible to reduce the response time to incidents, increase the efficiency of management decisions, and ensure the stability of the digital environment even under conditions of high turbulence.

Against the background of increasing cyber threats, the study of the relationship between the level of digital development, institutional readiness to counter risks, and AI capabilities has not only theoretical but also practical significance. In particular, the results of such a study could be used to form effective mechanisms for predicting and minimizing digital risks and devising a state strategy for forming a security-oriented digital space.

Thus, the justification and development of approaches to strengthening the economic security of the state using generative artificial intelligence is an important step towards adapting the national security system to the realities of the digital age and hybrid warfare. Therefore, research into minimizing digital risks and threats to the economic security of the state using generative artificial intelligence is relevant.

2. Literature review and problem statement

Paper [1] explores the potential of artificial intelligence in the digital economy. Despite the value of the general analysis, the paper lacks specific application recommendations for AI, in particular, it does not consider the use of generative models to increase the information resilience of digital systems; it does not consider the risks and vulnerabilities inherent in generative models themselves; it does not review standards, protocols, or technical practices that would facilitate the secure implementation of AI in government or corporate information systems. Possible reasons for such limitations are the authors' underestimation of the risks or potential of AI.

In [2, 3], the authors argue that AI can be a powerful tool for increasing the resilience of cyber-physical systems to covert attacks. However, in [2], the issue of practical implementation of generative AI in cyber defense systems is not resolved, which is mainly due to the strategic orientation of the research, while in [3], despite the presence of mathematical models for detecting hidden attacks in cyber-physical systems, the possibility of scaling solutions to the level of state or socio-economic systems is not considered, which is explained by the narrow focus of the work. The main difference between the works is in the level of analysis: [2] focuses on the conceptual and institutional aspects of ensuring economic security in the context of digitalization, while [3] demonstrates the applied use of generative models in the technical environment of cyber-physical systems, without going beyond the engineering paradigm.

The authors of [4] propose several methods for minimizing risks but ignore the impact of new technologies, such as generative AI, on these processes. The reason for not resolving this issue is that conventional protection methods are not adapted to modern threats. Works [5, 6] emphasize the importance of adequate assessment of cyber risks. However, the studies do not consider the use of new AI tools to automate risk assessment and integrate these technologies into corporate security strategies. The difference between these works is in the level of analysis and the object of the study: [5] focuses on the macro- and meso-levels (state and business policy in Ukraine), while [6] focuses on the organizational level (internal risk decision-making processes). Both works do not consider the potential of artificial intelligence as a tool for integrated assessment and management of cyber risks.

In [7], the authors propose the use of comprehensive preventive strategies to prevent cybercrime. However, they do not fully consider the impact of new technologies, such as generative AI, which allow attacks to become increasingly sophisticated.

The authors of [8] raise the issue of using AI to protect against cyber threats. They note that AI can become a powerful cybersecurity tool, but research does not provide a complete answer to the question of how exactly this could be implemented in the context of dynamic cyber threats.

Our review of the literature [1–8] reveals that there are a number of unresolved problems, in particular determining effective approaches to integrating AI into the national cybersecurity system, identifying relationships between the level of ICT development and cybersecurity.

Taking into account these gaps in research allows us to argue that it is advisable to conduct a comprehensive study aimed at identifying the patterns of the impact of digital transformation on the economic security of the state, identifying key risks and threats, and devising conceptual approaches to their neutralization using the capabilities of generative artificial intelligence.

3. The aim and objectives of the study

The purpose of our study is to identify the patterns of the impact of digital transformation on the economic security of the state through a comprehensive analysis of risks and threats associated with the development of information and communication technologies and the state of cybersecurity. This will make it possible to devise conceptual approaches to neutralizing digital risks and threats using generative artificial intelligence.

To achieve the goal, the following tasks were set:

– to investigate risks and threats to the economic security of the state in the field of digital transformation;

– to assess the relationship and interdependence between the level of development of information and communication technologies and the level of cybersecurity at the macro level;

– to substantiate conceptual approaches to strengthening the economic security of the state using generative artificial intelligence.

4. The study materials and methods

The object of our study is the process that provides for the economic security of the state under the conditions of digital transformation, which is accompanied by the growth of cyber threats and digital risks.

The principal hypothesis of the study assumes the presence of a statistically significant relationship between the level of ICT development and cybersecurity, as well as the effectiveness of using GAI to increase the resilience of the digital environment to destructive influences.

The study assumes that the state policy of digital development should integrate approaches to systematically counteracting the risks of digital transformation, and the use of GAI is able to ensure the preventive detection and neutralization of potential threats.

A set of interdisciplinary methods was used to conduct the study, in particular the risk analysis method and comparative analysis methods (employed to determine differences in the levels of ICT and cybersecurity development in 25 countries based on international index data). All calculations were carried out using open sources (E-Governance Academy, ITU); regression analysis was applied to build a mathematical model of the interdependence between the level of ICT development and the cybersecurity index. The model is constructed in the form of a linear equation with an estimate of the coefficient of determination, which makes it possible to assess the quality of explanation of variations in the dependent variable. The work used a graph-analytical method to visualize the gap between the levels of ICT and cybersecurity (GAP analysis) in the studied countries and identify countries with the largest positive and negative deviations. In addition, expert analysis was applied to formulate conceptual approaches to the implementation of GAI in the field of digital security, taking into account the results of case studies, organizational analytics, as well as the practices of Ukrainian structures and volunteer initiatives.

The methodological basis of our study is the principles of a systems approach, which allowed us to take into account the interrelationships between technical and technological, regulatory, institutional, and social factors of digital transformation. This provided a comprehensive vision of the impact of the digital environment on the economic security of the state.

5. Results of research on the determinants of minimizing digital risks and threats to the economic security of the state

5. 1. Modern risks and threats to the economic security of the state in the field of digital transformation

The digital transformation of the economy is accompanied by a number of risks of a regulatory, technological, security, and geopolitical nature, which have a complex impact on the economic stability of the state [9]. Generalization of official statistics, index estimates [10], reports by institutions [11], DREAM data [12], results of digital activity of enterprises [13] allowed us to identify the interdependence between digital maturity and the ability to adapt to turbulent conditions.

Based on the above, it is worth noting that critical regulatory threats include the lack of agreed regulatory standards for the exchange of digital data, the lack of regulation of the use of blockchain technologies, as well as a weak regulatory framework in the field of digital assets. In order to minimize the above threats, it is necessary to harmonize Ukrainian legislation with the EU regulatory framework, in particular in the areas of cybersecurity, electronic identification, and artificial intelligence [14].

In addition, during the research, significant technological barriers were identified, including the fragmentation of the digital market, insufficient digital maturity of the public sector, and limited ability to scale innovative solutions. It was also found that the automation of big data collection and processing is slow, which complicates real-time decision-making, reducing the adaptability of the economy [15]. In the field of digital security, there is an increase in risks due to both the growth of cyber threats and the lack of sustainable countermeasures. Increased vulnerability is demonstrated by critical digital infrastructure, which suffered direct losses in the amount of more than USD 510 million as a result of full-scale armed aggression [11]. It was also recorded that 11% of mobile base stations stopped working, which significantly reduces the stability of digital communications at the regional level.

In the context of martial law, the digitalization of the economy plays the role of a compensatory mechanism for economic development [16]. Thus, a significant number of Ukrainian enterprises continue to invest in digital technologies, in particular in artificial intelligence, cloud computing, and telecommunications solutions [17]. At the same time, our study identified a need for modernization of industry, development of domestic production of high-tech products, and development of digital competencies in the workforce. At the strategic level, it was recorded that Ukraine demonstrates positive dynamics of digital governance. The e-government development index increased from 0.8029 in 2020 to 0.8841 in 2024 [18], which indicates the gradual implementation of digital solutions in the provision of public services. However, threats to digital security remain critical due to geopolitical instability, which limits integration into the EU single digital market.

In general, the results of our study indicate the need for a systemic state policy in the field of digital security and targeted integration of digital strategies into general economic policy. Analysis of the identified risks of digital transformation [19] allowed us to establish a systemic interdependence between the level of technological readiness, the effectiveness of the regulatory environment and national economic security. Thus, in regions with a higher level of digitalization, there is a higher dynamics of attracting investment resources, more efficient business functioning, as well as less dependence on external digital service providers. This indicates the potential of digital technologies as a factor of economic stability in times of crisis.

At the same time, cybersecurity threats remain one of the most destabilizing factors. The convergence of artificial intelligence and quantum computing technologies creates risks that do not have conventional neutralization mechanisms, which requires the development of new concepts of cyber protection at the state policy level [20]. Special attention is required to develop the ability to predict and counter cyberattacks aimed at critical infrastructure facilities – energy, transport, telecommunications, and finance.

Our study also revealed a high degree of dependence of economic security on the level of digital inclusion of people. Limited access to digital services in a number of regions of Ukraine leads to increased socio-economic inequality, which is one of the latent risks of destabilizing state policy. Digital inequality deepens the territorial asymmetry of development, reduces the effectiveness of e-governance, and complicates the mobilization of resources in crisis situations.

Analysis of institutional factors [21] revealed that economic security in the context of digital transformation largely depends on the ability of the state to ensure coordinated interaction between government agencies, businesses, and civil society. The potential of the DREAM digital ecosystem, which aggregates more than 7 thousand investment projects [12], demonstrates the effectiveness of digital tools as a platform for intersectoral cooperation, but requires increased transparency and independent monitoring mechanisms.

In the context of Ukraine's European integration course, the key challenge is the need to harmonize national digital policy with the requirements of the European digital market [22]. The key parameters of such integration should be mutual recognition of trust services, digital identity, electronic signatures, as well as compliance with European

requirements in the field of data protection and regulation of artificial intelligence.

Thus, our results indicate that digital transformation is not only a source of new economic opportunities but also a critical area of risks that can undermine the stability of the national economy under conditions of multi-vector instability. This requires a strategic rethinking of the role of digitalization in the system of economic security of the state.

5. 2. Assessing the relationship and interdependence between the level of development of information and communication technologies and the level of cybersecurity

The assessment of the relationship and interdependence between the level of development of information and communication technologies and the level of cybersecurity at the macro level was carried out using a combination of statistical methods and data from official international indices.

The National Cybersecurity Index is an aggregated indicator used to assess the level of readiness of a country to prevent cyber threats and manage cyber incidents. The index forms a quantitative measurement system based on open data and serves as a tool for strategic planning for the development of national potential in the field of cybersecurity. Its structure allows for cross-country comparison without ranking, which contributes to the formation of a holistic picture of the state of cyber defense without creating a competitive environment [23].

The ICT Development Index is an integrated indicator that reflects the level of development of digital infrastructure and access to ICT in the country under study [24]. The index involves assessment according to a system of indicators of ICT accessibility, use and quality, and does not involve the formation of a country rating. This approach provides analytical accuracy and makes it possible to track the dynamics of digital transformation, taking into account the regional and socio-economic context.

The above indices measure various aspects of the digital environment; their combination in the study makes it possible to comprehensively assess the balance between the level of technological development and the country's readiness for cyber threats. Therefore, we can put forward a hypothesis that there is a statistically significant relationship between the level of ICT development and the level of cybersecurity in the country. At the same time, the presence of a high level of ICT does not guarantee an adequate level of cyber protection without a targeted state policy in the field of cybersecurity. To test this hypothesis, we shall use a set of statistical research methods.

A comparative analysis of the level of development of information and communication technologies and the level of cybersecurity of countries is illustrated in Table 1.

The countries with the highest level of cybersecurity include Belgium (94.81), Lithuania (93.51), Estonia (93.51), the Czech Republic (90.91), and Germany (90.91). These countries have developed national strategies, institutions, and technological mechanisms for cyber protection. Ukraine lags behind in terms of cybersecurity (75.32) despite high indicators of the level of ICT development. The leaders in terms of the level of development of information and communication technologies are Finland (98.1), Estonia (97.9), Denmark (97.1), Poland (95.8), Lithuania (94.2) – countries with a high level of digitalization of society and economy. At the same time, in some of them (for example, Sweden – GAP: 10.88) the level of cybersecurity lags behind ICT development. In a number of countries (Portugal, Greece, Romania), a positive deviation (GAP > 0) is observed, which indicates the priority of cybersecurity development even with a relatively lower level of ICT development. In countries with a high level of ICT development and a low level of cybersecurity (Italy, Estonia, Poland), there is a need to strengthen cyber protection to ensure digital resilience.

Table 1

Comparative analysis of the level of development of information and communication technologies and the level of cybersecurity in countries

No.	Country	National Cybersecurity Index (NCSI) in 2024	Information and Communication Technologies development index (ICT)			GAP (NCSI-ICT) in 2024
			2023	2024	Change, %	
1	Belgium	94.81	88.2	89.3	+1%	5.51 ↑
2	Lithuania	93.51	92.4	94.2	+2%	–0.69 ↓
3	Estonia	93.51	96.9	97.9	+1%	–4.39 ↓
4	Czech Republic	90.91	86.1	88.0	+2%	2.91 ↑
5	Germany	90.91	87.3	87.8	+1%	3.11 ↑
6	Romania	89.61	87.0	87.6	+1%	2.01 ↑
7	Greece	89.61	83.7	86.5	+3%	3.11 ↑
8	Portugal	89.61	85.6	87.4	+2%	2.21 ↑
9	United Kingdom	89.61	92.8	93.6	+1%	–3.99 ↓
10	Spain	88.31	91.4	92.5	+1%	–4.19 ↓
11	Poland	87.01	94.6	95.8	+1%	–8.79 ↓
12	Austria	85.71	92.5	94.3	+2%	–8.59 ↓
13	Finland	85.71	96.7	98.1	+1%	–12.39 ↓
14	Saudi Arabia	84.42	94.9	95.7	+1%	–11.28 ↓
15	France	84.42	89.4	89.8	+0%	–5.38 ↓
16	Sweden	84.42	93.9	95.3	+1%	–10.88 ↓
17	Denmark	84.42	96.9	97.1	+0%	–12.68 ↓
18	Croatia	83.12	87.1	89.6	+3%	–6.48 ↓
19	Slovakia	83.12	87.1	87.1	+0%	–3.98 ↓
20	Netherlands	83.12	93.5	92.5	–1%	–9.38 ↓
21	Serbia	80.52	85.1	87.7	+3%	–7.18 ↓
22	Malaysia	79.22	94.5	95.0	+1%	–15.78 ↓
23	Italy	79.22	86.4	87.7	+2%	–8.48 ↓
24	Ukraine	75.32	80.8	81.0	+0%	–5.68 ↓
25	Latvia	75.32	93.8	94.3	+1%	–18.98 ↓
↑	The level of cybersecurity is higher than the level of development of information and communication technologies in the country		↓	The level of cybersecurity is lower than the level of development of information and communication technologies in the country		

Source: compiled by authors based on data from the E-Governance Academy and the International Telecommunication Union.

Countries with a high level of information and communication technologies development but a low level of cybersecurity are vulnerable to cyber incidents, which can undermine trust in digital services and restrain digital transformation. Conversely, countries with a high level of cybersecurity, even with an average level of information and communication technologies development, demonstrate a proactive state policy to ensure a safe digital environment.

The comparative dynamics of deviations between the level of ICT development and the level of cybersecurity in the studied countries are shown in Fig. 1, which makes it possible to identify countries with the highest positive and negative gaps between the level of ICT development and the level of cybersecurity.

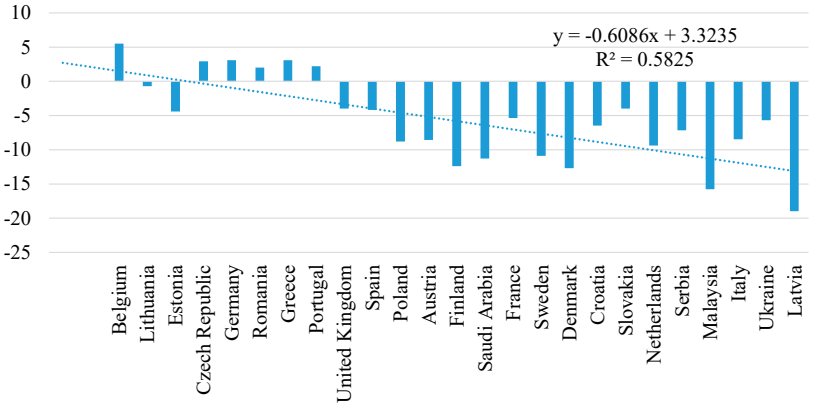

Fig. 1. Analysis of the gap between the level of development of information and communication technologies and the level of cybersecurity of countries

The constructed regression model of the dependence of GAP on the level of ICT development takes the form

$$y = -0.6086x + 3.3235, \quad (1)$$

where y is the gap between NCSI and ICT; x is the value of ICT.

The value of the coefficient of determination $R^2 = 0.5825$ indicates that 58.25% of the variation in the gap is explained by the level of ICT development. The resulting negative value of the slope coefficient (–0.6086) confirms the presence of a feedback loop: the higher the level of digital development, the less likely it is that the level of cybersecurity will be higher. This pattern may be a consequence of the fact that the rapid implementation of ICT is not always accompanied by adequate investments in security.

The graphical method allowed us to identify clusters of countries with different levels of correspondence between ICT infrastructure and the effectiveness of cyber security measures. The following patterns were identified as a result:

1. Countries with a high level of ICT and cybersecurity (Great Britain, Finland, the Netherlands) have a high level of cyber power, which is manifested through balanced investment in digital infrastructure and protective mechanisms.

2. Countries with an imbalance – with a high level of ICT, but a relatively low level of cybersecurity (France, Italy, Latvia) – are potentially vulnerable to cyber attacks. This situation indicates insufficient strategic integration of information security policy into digital development.

3. Countries with low ICT and cybersecurity are usually focused on basic digital technology development needs and only fragmentarily integrate cyber defense components. Their cyber capacity is minimal, which makes them vulnerable to external threats. Countries with low ICT and cybersecurity are mostly focused on building primary digital infrastructure, with little emphasis on the security component. Their efforts are focused on the availability of ICT in basic areas (education, healthcare, public services), but the lack of a systemic vision of cybersecurity makes it difficult to ensure digital resilience.

Ukraine is closer to the average level in both indicators but demonstrates increasing dynamics in the field of cybersecurity. In the context of a prolonged large-scale war by the Russian Federation, the presence of a strategically sound cyber defense policy is critically important. Ukraine's cyber defense strategy, which focuses on strengthening digital resilience, building a national cyber center, and developing partnerships with international structures, is justified in the context of an external threat. Ukraine's cyber power is manifested in the following key areas [25]:

– development of specialized cyber troops;

– activation of cyber volunteer initiatives;

– introduction of regulatory acts in the field of cyber defense;

– cooperation with NATO and EU countries in the field of cybersecurity.

Particular attention is drawn to a group of countries in which the level of cybersecurity significantly exceeds the level of digital development (Belgium, the Czech Republic, Germany), which indicates the presence of a priority cyber defense policy at the level of the national economy, regardless of the development of digital infrastructure. On the other hand, in countries with the largest negative deviation (Latvia, Malaysia, Denmark, Sweden), an imbalance is observed, which may be associated with an underestimation of risks in the field of information security against the background of the rapid introduction of digital technologies in the country. Thus, the results of our analysis make it possible not only to characterize the current state of cyber power of countries but also identify vectors of strategic development in the field of digital security.

5. 3. Substantiation of conceptual approaches to strengthening the economic security of the state using generative artificial intelligence

The full-scale Russian-Ukrainian war has led to the transformation of modern approaches to ensuring the economic security of the state, in particular in terms of responding to cyber threats. One of the innovative vectors for enhancing cyber resilience is the integration of generative artificial intelligence into digital security systems, which opens up new opportunities for preventive analysis, adaptive protection, and proactive threat identification.

Based on the approaches to defining GAI, structured in Table 2, it is worth stating that generative artificial intelligence is a class of intelligent algorithmic systems that are capable of creating new, previously non-existent digital objects based on the analysis of large arrays of structured and unstructured data, in order to increase the stability of the information environment and prevent the destructive impact of digital risks on the economic security of the state. Within the concept of security-oriented digital transformation, GAI acts as a multifunctional tool for proactive threat analysis, automated construction of response scenarios, adaptive anomaly

detection, and support for management decision-making processes in real time.

Table 2

Basic approaches to defining generative artificial intelligence

Approach to defining GAI	Key ideas	Source
GAI as a driver of a new wave of digital transformation, capable of generating new economic values by creating content, decision models and digital products	GAI is considered as a component of the data economy that expands human capabilities	[1]
GAI is considered as a potential element of cyber-physical systems, which can both enhance and complicate protection against hidden attacks	Focus on GAI vulnerabilities in management systems, the need for robust control mechanisms	[3]
GAI is considered as a decision-making tool that changes the perception of risks	The impact of GAI on scenario-based risk modeling, in particular in cyberspace	[6]
GAI is considered as part of cybercrime prevention through the analysis of behavioral patterns	GAI as a tool in the mechanisms of situational prevention of cyber threats	[7]
GAI is a new battlefield in the field of cybersecurity, generating both new opportunities and new threats (automated attacks, deep learning of attackers)	The dual nature of GAI: a tool for protection and attack	[8]
GAI is as an algorithmic forecasting model in markets, capable of creating scenarios based on big data	The use of GAI in forecasting economic indicators	[26]
GAI is as a comprehensive tool for solving engineering, medicine, and industry problems by generating new solutions	GAI as a cross-sector driver of innovation, in particular for sustainable development	[27]

Source: compiled by Authors based on data from [1, 3, 6–8, 26, 27].

Our research and generalization of the features of the manifestation of destructive factors of economic security in the information sphere make it possible to systematize practical cases of the use of GAI in cyberspace. In particular, the use of malicious software generated with the involvement of GAI for attacks on the IT sector, energy companies, and state institutions of the enemy was recorded, which indicates the potential of such technologies in the deformation of enemy infrastructure. In parallel, Horizon3.ai specialists and other specialized organizations presented GAI-based systems that demonstrate the ability to highly accurate identification of vulnerabilities and effective prioritization of response measures. In light of the results, it is worth systematizing the main areas of minimizing digital risks in Ukraine and abroad, which are given in Table 3.

The approaches presented in it demonstrate the need for multi-level integration of generative artificial intelligence into the digital ecosystem of the state – from analytical tools to regulatory regulation and educational training. This approach makes it possible to ensure compliance between the complexity of the latest cyber threats and the effectiveness of digital security tools, forming the basis for sustainable development under conditions of multi-vector turbulence.

In order to minimize digital risks and threats to the economic security of the state using generative artificial intelligence, a conceptual model has been proposed that includes the following structural modules:

1. Analytical and predictive module, which involves the use of generative artificial intelligence to predict cyber threats based on the analysis of large volumes of open data, attack telemetry, pentest results, and digital behavior metadata.

2. Infrastructure and technical module, focused on embedding generative artificial intelligence models into the architecture of digital systems with fundamental adherence to the Secure by Design and Zero Trust Architecture approaches.

3. A regulatory and legal module, consistent with the provisions of the European Act on Artificial Intelligence, regulating the cyber resilience of AI systems.

4. An educational and competence module, covering the creation of cyber training infrastructure, such as national cyber training grounds and cyber defense laboratories, with a focus on generative models.

5. A coordination and institutional module, providing for the integration of national and international institutions (in particular ENISA, CISA) into the process of forming strategies for the use of AI.

Table 3

Directions for minimizing digital risks in Ukraine and the world

Direction of minimization of digital risks	Ukrainian context	Global context	Expected effect
Analytical and prognostic modeling of risks using GAI	DREAM platforms, situational centers, open source cyber analysis	Horizon3.ai, IBM Watson, MITRE ATT&CK	Reduced time to detect threats, adaptive response
Infrastructure modernization	Implemented in defense and finance, limited in the civilian sector	Widely used in the US, Estonia, Singapore, Israel	Enhanced cyber resilience and reliability of government and corporate systems
Harmonization of the normative and legal field	Laws on cybersecurity, critical infrastructure; no separate policy on GAI	EU AI Act, GDPR, NIS2	Legal certainty, compliance with European requirements, reduced legal risks
Formation of the educational and competence ecosystem	Cyber labs in HEIs, online platforms of the Ministry of Digital Affairs	AI4Sec (US), Digital Europe (EU), CyberEDU (Canada) programs	Strengthening digital competencies, increasing inclusion
Institutional coordination and intersectoral interaction	NSDC, volunteer initiatives; fragmented business participation	CISA, ENISA, NATO, NCFTA	Coordinated response, knowledge exchange between sectors
Technological implementation environment for GAI	Testing in energy, logistics, security analytics	Integrated solutions from Google, Microsoft	Transition to proactive cyber defense, narrowing the gap between attack and response

Source: compiled by Authors based on data from [3, 7, 26].

The key factor in the effectiveness of the implementation of this model is the development of human capital and the creation of an intersectoral ecosystem of interaction between the state, business, academic structures, and civil society. At the level of policy implementation, it is relevant to initiate the development of a national strategy for the use of GAI in the digital security sector, by analogy with the US Strategy 2024 [28].

In order to ensure economic security, it is important to pay special attention to identifying weaknesses in the cyber protection system of critical infrastructures, the banking sector, healthcare facilities, media, and supply chains [29, 30]. It is necessary to adapt GAI to the tasks of automated monitoring and independent detection of anomalies in digital flows, which makes it possible to significantly reduce the response time to incidents and increase overall cyber resilience.

Therefore, conceptual approaches to strengthening economic security using GAI involve a set of measures to transform organizational structures, technological content, and regulatory regulation in the direction of building a cyber defense model adapted to war.

6. Discussion of results based on the study on minimizing digital risks and threats to the economic security of the state using artificial intelligence

The systematic identification of the risks of digital transformation made it possible to establish that regulatory fragmentation, low digital maturity of the public sector, and weak cyber protection mechanisms are key determinants of the decline in economic sustainability. This is confirmed by direct losses of critical digital infrastructure worth over USD 510 million [11], as well as partial loss of mobile communications at the regional level.

The constructed model of interdependence between the level of ICT development and the level of cybersecurity (Fig. 1, Table 1) explains the paradox of digital vulnerability even in countries with a high level of digitalization. The derived regression equation and $R^2 = 0.5825$ confirm that the rapid development of ICT does not guarantee the growth of cybersecurity without strategic institutional support. For example, countries such as Poland, Latvia, and Denmark, which have a high level of ICT (>94), demonstrate a negative GAP of more than −8, which indicates a systemic underestimation of information security risks.

A conceptual model of integrating GAI into the digital security system has been proposed. Within the framework of the conceptual analysis, the main approaches to defining GAI were systematized, given in Table 2, which allowed us not only to generalize the interpretation of GAI (as a tool for digital transformation, a component of cyber-physical systems, a tool for behavioral analytics) but also justify the feasibility of its use as an element of the strategic architecture of digital security. Particular attention is drawn to such aspects as the dual nature of GAI (at the same time a tool for attack and defense), its role in scenario modeling and risk analysis, as well as functions in the analysis of digital behavior. The systematization of approaches allowed us to clarify the functional load of each of the modules of the proposed model and ensure interdisciplinary consistency of the proposed solution.

Empirical examples (Table 3) demonstrate that Ukraine is already using AI in open source analysis systems (DREAM), defense solutions, as well as in the educational domain (cyber labs). In the global context, examples of Horizon3.ai, IBM indicate the scaling of AI technologies for operational threat detection and rapid adaptation of security strategies.

The advantages of the solutions proposed in our study are their innovation and holistic nature. In particular, the conceptual model of integrating generative artificial intelligence into the field of digital security has a multi-level architecture, including analytical and predictive, infrastructure and technical, regulatory, and legal, educational and competency-based, and coordination and institutional modules. Unlike conventional approaches that focus mainly on passive protection, the proposed model provides proactive forecasting, detection, and neutralization of threats based on big data and telemetry.

In addition, the advantage is the focus on generative models that are able not only to detect anomalies but also adaptively update their own algorithms in real time. For example, based on the experience of Horizon3.ai, GAI models demonstrate effectiveness in prioritizing risks and automating incident response, which reduces the response time to cyberattacks by 30–50% [26]. This creates the prerequisites for the transformation of digital security strategy from reactive to preventive.

Unlike [2], where the emphasis is on the use of generative AI mainly for detecting vulnerabilities in cyber-physical systems under laboratory conditions, the model proposed in our study has a practical orientation and is adapted to the conditions of strategic management at the level of state digital policy. This has been made possible by integrating generative models into five functional modules (analytical, infrastructural, normative, educational, institutional), covering both technological and organizational-institutional dimensions of economic security.

Compared to the approaches presented in [4], where the main focus is on minimizing cyber risks through conventional monitoring and log analysis methods, the proposed model provides proactive threat prediction based on digital behavior and adaptive learning of GAI.

Unlike study [7], which considers preventive strategies mainly from the perspective of criminological prevention, our work demonstrates the synergy between the technological tools of GAI and intersectoral security management mechanisms. In particular, the implementation of the modules of digital competence and institutional coordination makes it possible not only to reduce risks but also ensure the scalability of the proposed solutions in different sectors of the economy.

Also, unlike [8], where AI is considered as a separate tool of cyber protection without inclusion in the overall architecture of digital security, in the proposed concept GAI acts as a system-forming element that interacts with open data, cyber regulation, and digital inclusion. This makes it possible to achieve not only the technical but also the institutional effect of strengthening economic security.

In addition, the proposed model provides for compliance with the provisions of the European Act on Artificial Intelligence, which is not provided for by the models presented in [1], where generative systems are analyzed without a regulatory context. The model takes into account the need for legitimacy and ethics in the use of GAI in critical areas, which is becoming a determining factor in the process of Ukraine's European integration.

The results of our study, in particular, the construction of a model of the relationship between the level of ICT development and cybersecurity, the identification of an imbalance between digital development and the level of protection, as well as the development of a five-module conceptual model of GAI integration, allow us to resolve the problems related to insufficient resilience of the digital infrastructure and the fragmentation of cyber protection. In particular, it was proven that the integration of GAI into the key contours of digital security management ensures adaptability to new types

of threats, in particular those based on the convergence of quantum technologies and generative artificial intelligence. The proposed model achieves alignment with the European Act on Artificial Intelligence [30], which ensures regulatory compatibility within the EU Digital Single Market.

At the same time, it is necessary to note certain limitations of our study. First, the empirical basis of the study is based on official open data, which may not take into account indicators, in particular at closed military-industrial facilities. In addition, further testing of the GAI model in a real-time environment is necessary to verify its resistance to attacks such as adversarial AI, etc. The shortcomings of the study are that we did not cover the ethical dilemmas of using GAI in critical systems – an issue that requires further interdisciplinary analysis.

Possible areas for future studies are:

– adaptation of the proposed model to the needs of the healthcare, energy, and logistics sectors;

– development of a digital certification system for solutions based on GAI;

– modeling scenarios for synchronization of national cyber policy with the requirements of CISA (USA), ENISA (EU);

– construction of hybrid systems based on GAI and edge computing to ensure local response in crisis zones.

These vectors are key to ensuring a dynamic match between the growing complexity of cyber threats and the effectiveness of digital security tools.

7. Conclusions

1. Our study of risks and threats to the economic security of the state in the field of digital transformation showed that the main threats are cyberattacks, infrastructure vulnerabilities, and the lack of preparedness of organizations to quickly adapt to new technologies. In particular, it was found that as a result of the full-scale armed aggression of the Russian Federation against Ukraine, critical digital infrastructure suffered losses of more than USD 510 million, and 11% of mobile communication base stations in Ukraine ceased to function, which destabilizes digital economic processes. It was found that risks are increasing due to the insufficient level of state control over digital platforms and transformation processes. The solution to some of these threats is to improve the legislative framework, as well as increase the level of preparedness of human resources to respond to these risks, which would reduce the likelihood of negative consequences in the medium term.

2. The assessment of relationship between the level of development of information and communication technologies and the level of cybersecurity at the macro level revealed the presence of a statistically significant inverse relationship ($r = -0.763$, $p < 0.05$), indicating a potential technological imbalance: the growth of ICT without a corresponding strengthening of cyber defense increases the vulnerability of digital systems. Regression analysis ($R^2 = 0.5825$) confirmed that 58.25% of the variations in the gap between the level of ICT and cybersecurity are explained by the level of digital development. Countries such as Poland, Latvia, Denmark, and Malaysia demonstrate a negative gap (GAP from –8 to –18), which indicates the need to strengthen cyber potential even in digitally developed countries. Therefore, the strategic integration of ICT and cyber defense policies is critically important for ensuring the economic security of states.

3. Substantiation of conceptual approaches to strengthening the economic security of the state using generative artificial intelligence has proven that the integration of GAI into the digital security system provides a significant increase in the level of adaptability to threats. The practical implementation of such solutions makes it possible to reduce the response time to cyberattacks by 30–50% due to automated vulnerability detection and risk prioritization. The proposed GAI model includes five functional modules (analytical, technical, regulatory, educational, and institutional), which cover the full range of threats in the digital environment. The experience of Horizon3.ai, DREAM analytics, as well as analysis of the Ukrainian cyber sector, confirm the advantages of generative models in ensuring cyber resilience. The implementation of GAI into national security systems is extremely important for strengthening the economic security of the state in the context of digital transformation.

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. Hang, H., Chen, Z. (2022). How to realize the full potentials of artificial intelligence (AI) in digital economy? A literature review. Journal of Digital Economy, 1 (3), 180–191. https://doi.org/10.1016/j.jdec.2022.11.003
2. 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/10.15587/1729-4061.2025.319256
3. Griffioen, P., Krogh, B. H., Sinopoli, B. (2024). Ensuring Resilience Against Stealthy Attacks on Cyber-Physical Systems. IEEE Transactions on Automatic Control, 69 (12), 8234–8246. https://doi.org/10.1109/tac.2024.3401013

4. Birthriya, S. K., Ahlawat, P., Jain, A. K. (2024). A Comprehensive Survey of Social Engineering Attacks: Taxonomy of Attacks, Prevention, and Mitigation Strategies. Journal of Applied Security Research, 20 (2), 244–292. https://doi.org/10.1080/19361610.2024.2372986
5. Yanko, A., Hlushko, A., Onyshchenko, S., 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
6. Parkin, S., Kuhn, K., Shaikh, S. A. (2023). Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception. Journal of Cybersecurity, 9 (1). https://doi.org/10.1093/cybsec/tyad018
7. Ho, H., Ko, R., Mazerolle, L., Gilmour, J., Miao, C. (2024). Using Situational Crime Prevention (SCP)-C3 cycle and common inventory of cybersecurity controls from ISO/IEC 27002:2022 to prevent cybercrimes. Journal of Cybersecurity, 10 (1). https://doi.org/10.1093/cybsec/tyae020
8. Khan, K., Khurshid, A., Cifuentes-Faura, J. (2024). Is artificial intelligence a new battleground for cybersecurity? Internet of Things, 28, 101428. https://doi.org/10.1016/j.iot.2024.101428
9. 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
10. Network Readiness Index 2024. Portulans Institute. Available at: https://networkreadinessindex.org/
11. Report on direct damages to infrastructure due to Russia's military aggression against Ukraine as of early 2024 (2024). Kyiv School of Economics. Available at: https://kse.ua/wp-content/uploads/2024/04/01.01.24_Damages_Report.pdf
12. Digital Restoration Ecosystem for Accountable Management (DREAM) (2024). Ministry for Communities, Territories and Infrastructure Development of Ukraine. Available at: https://dream.gov.ua
13. Indeks tsyfrovoi transformatsiyi rehioniv Ukrainy. Pidsumky 2024 roku. Ministerstvo tsyfrovoi transformatsiyi Ukrainy. Available at: https://thedigital.gov.ua/storage/uploads/files/page/community/reports/%D0%86%D0%9D%D0%94%D0%95%D0%9A%D0%A1%202024%202%201.pdf
14. Onyshchenko, V., Onyshchenko, S., Verhal, K., Buriak, A. (2023). The Energy Efficiency of the Digital Economy. Proceedings of the 4th International Conference on Building Innovations, 761–767. https://doi.org/10.1007/978-3-031-17385-1_64
15. Ponochovniy, Y., Bulba, E., Yanko, A., Hozbenko, E. (2018). Influence of diagnostics errors on safety: Indicators and requirements. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 53–57. https://doi.org/10.1109/dessert.2018.8409098
16. Maslii, O., Maksymenko, A. (2025). Digital transformation and economic deindustrialisation: impact on state financial security. Financial and Credit Activity Problems of Theory and Practice, 1 (60), 401–414. https://doi.org/10.55643/fcaptp.1.60.2025.4599
17. Chychkalo-Kondratska, I., Buriak, A. (2014). Factors of foreign direct investment attracting into economy of Ukraine's regions. Economic Annals-XXI, 11-12, 88–92. Available at: https://ea21journal.world/index.php/ea-v146-22/
18. E-Government Development Index 2024. United Nations. Available at: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/185-Ukraine
19. 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
20. Krasnobayev, V., Yanko, A., Kovalchuk, D. (2023). Control, Diagnostics and Error Correction in the Modular Number System. Computer Modeling and Intelligent Systems, 3392, 199–213. https://doi.org/10.32782/cmis/3392-17
21. 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
22. Onyshchenko, S., Hlushko, A., Kivshyk, O., Sokolov, A. (2021). The shadow economy as a threat to the economic security of the state. Economics of Development, 20 (4). https://doi.org/10.57111/econ.20(4).2021.24-30
23. National Cyber Security Index. E-Governance Academy. Available at: https://ncsi.ega.ee
24. Measuring digital development – ICT Development Index 2024. International Telecommunication Union. Available at: https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-3/
25. 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. Available at: https://scibulcom.net/en/article/L8nV7It2dVTBPX09mzWB
26. Kadam, S., Agrawal, A., Bajaj, A., Agarwal, R., Kalra, R., Shah, J. (2023). Predicting Crude Oil Future Price Using Traditional and Artificial Intelligence-Based Model: Comparative Analysis. Journal of International Commerce, Economics and Policy, 14 (03). https://doi.org/10.1142/s179399332350014x
27. Asvial, M., Zagloel, T. Y. M., Fitri, I. R., Kusrini, E., Whulanza, Y. (2023). Resolving Engineering, Industrial and Healthcare Challenges through AI-Driven Applications. International Journal of Technology, 14 (6), 1177. https://doi.org/10.14716/ijtech.v14i6.6767
28. E-Government Development Index (EGDI). United Nations. Available at: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index
29. Creemers, R. (2022). China's emerging data protection framework. Journal of Cybersecurity, 8 (1). https://doi.org/10.1093/cybsec/tyac011
30. Kravets, I. V., Mykhalchenko, H. H., Buriak, A. A., Davidyuk, L. P., Dubych, C. V. (2020). Long-term consequences of capital outflows for transition countries. International Journal of Management, 11 (5), 1017–1026. Available at: https://ssrn.com/abstract=3631765