Impact of Digitalization and the Changing Security Environment on the Transformation of the Functioning Mechanism of Business Entities

Natalia Lagodiienko
D.Sc., Prof.,
Higher Education Institution
International University of Business and Law,
Mykolaiv, Ukraine
besedina77@gmail.com

Bohdan Fishchuk
PhD Student,
Chernihiv Polytechnic National University,
Chernihiv, Ukraine
fishchukbohdan@yahoo.com

Igor Zoshchuk
PhD Student,
Chernihiv Polytechnic National University,
Chernihiv, Ukraine
ihor.zoschuk@gmail.com

Nazarii Fishchuk
PhD Student,
Chernihiv Polytechnic National University,
Chernihiv, Ukraine
nfishchuk@yahoo.com

Dmytro Kryvko
PhD Student,
Chernihiv Polytechnic National University,
Chernihiv, Ukraine
kryvkodmytro89@gmail.com

Abstract

The study is aimed at substantiating and evaluating the transformation of the mechanism of functioning of business entities under the impact of digitalization and the changing security environment. The methodological basis is a system and comparative approaches, statistical generalization, min-max normalization, integral assessment, weighting and ranking. The empirical base is formed based on the data of the Czech Republic, Hungary, Poland, Romania and Bulgaria, which are comparable in terms of institutional conditions of within the EU functioning, at the same time differ in the level of digital maturity of enterprises. For the comprehensive characterization of transformation processes, the indicators are grouped into three interrelated areas, namely: the level of digitalization, personnel and organizational transformation, and the security aspect of digitalization. The generalization of these components was carried out using the Comprehensive Index of Digital Transformation of Business Entities (CIDT). The main results of the study showed a significant differentiation of countries in terms of the level of digital transformation of the functioning mechanism of enterprises. The highest result was obtained by the Czech Republic – CIDT=0.780, which characterizes the highest and most balanced level of digital transformation. Hungary (0.520) and Poland (0.465) formed a group with an average level, but demonstrated different internal profiles: Hungary is characterized by high human and organizational capacity, while Poland is defined as a key constraint by the insufficient level of the security component. Romania (0.383) took the fourth position, demonstrating the highest security component among the studied countries with a lower level of technological digitalization. Bulgaria (0.128) is characterized by a low level of digital transformation and a systemic lag in terms of technological and personnel-organizational components. The practical effect of the study is to identify differentiated priorities of digital transformation: for the Czech Republic – maintaining a comprehensive balance; for Hungary – technological deepening and strengthening of digital security; for Poland – the priority of the development of cybersecurity mechanisms; for Romania – acceleration of technological

digitalization based on the established security base; for Bulgaria – comprehensive build-up of digital and personnel and organizational capacity.

Keywords: Digitalization, Digital Transformation, Business Entities, Functioning Mechanism, Digital Security, Personnel Transformation, Security Environment, Adaptability, Integral Index, CIDT.

Introduction

Digitalization is one of the key factors in the transformation of the modern business environment, changing the way of the production and management processes, which are organized, interacting with employees and customers, using information and making managerial decisions. For business entities, digital technologies create opportunities to increase operational efficiency, flexibility and competitiveness, while at the same time creating new requirements for staffing, organizational structure and protection of digital resources. The relevance of digital transformation is enhanced by the variability of the external environment of enterprises, which is characterized by economic uncertainty, technological changes, geopolitical and military risks, cyber threats, infrastructure restrictions and disruptions of established supply chains. Under these conditions, digitalization acquires a dual character: on the one hand, it is a tool for adapting enterprises to changes, and on the other hand, it creates new dependencies and vulnerabilities related to the use of digital infrastructure, data and information systems.

At the same time, the existing approaches to assessing digital transformation often focus mainly on the technological component, leaving personnel, organizational and security aspects out of the comprehensive assessment. This necessitates the formation of the integrated approach that allows assessing the technological readiness of enterprises, their ability to organizationally implement digital changes, and the ability to ensure safe functioning within the external risks.

Literature Review

The digital transformation of business entities in modern conditions is considered not only as introducing individual information and communication technologies, but as a complex change in the ways of organizing business processes, resource management, decision-making, and interaction with the external environment. Studies of the digital transformation of business processes emphasize the need to restructure the mechanisms of their management and coordination, while modern works on digital business focus on changing the ways of creating and developing the economic value (Kirchmer (2021); Leimstoll et al. (2018). Digital maturity models further show that digital transformation should be characterized not only by the availability of technologies, but also by the depth of their integration into operational and management processes (Han et al. (2025)).

An important aspect is the transition from fragmented digitalization of individual operations to systemic transformation of business models and processes. Kirchmer (2021) considers digital transformation through the prism of business process management, while Leimstoll et al. (2018) associate it with the development of e-business and new ways of organizing activities. The study of digitalization of business processes in the context of the increased global competition also indicates its importance for changing the competitive capabilities of enterprises (Ostrovska et al. (2023)). In the Ukrainian context, digital transformation is considered as a source of new opportunities for business development and modernization of economic processes (Kalenyuk et al. (2025)). At the same time, the regulatory environment is an important prerequisite for the development of digital business, as it determines the institutional conditions for the implementation of digital solutions.

The separate area of the research is formed by works in which digital transformation is associated with the development of human and organizational potential. Browder et al. (2024) show that digital transformation can enhance organizational resilience through the development of digital capabilities, including virtual access, digital collaboration, data-driven decision-making, and algorithmic reprogramming. Awad and Martín-Rojas (2024) link digital transformation and organizational resilience to organizational learning and innovation. The importance of human capital for economic dynamics is also

confirmed by the research of Derii et al. (2022), while the role of intellectual capital in the innovative development of enterprises within the digitalization is revealed by Hryhoruk et al. (2024). The development of artificial intelligence and digital technologies also increases the requirements for human capital, education, and competencies (Lagodiienko et al. (2025)). In a broader context, digital transformation is associated with the innovative development of enterprises and economic systems, as well as with the formation of strategies for the sustainable development of companies.

The important context of the research is the relationship between digital transformation and enterprise resilience. Li and Wang (2024), based on data from Chinese companies, showed a positive impact of digital transformation on the resilience of enterprises, linking this effect to reduced agency costs, increased information transparency, and easing financial constraints. Xu et al. (2024a) established a positive relationship between digital transformation and the ability of enterprises to withstand supply chain disruptions, with the effect enhanced by supplier diversification and geographic diversification. Xu et al. (2024b) also found a positive impact of digital transformation on enterprise resilience through green innovation and overall factor productivity channels. At the same time, Wang et al. (2025) showed that the relationship between digital transformation and corporate resilience can be non-linear, so further scaling up digitalization does not guarantee a proportional increase in resilience. In addition, the resilience of enterprises is associated with inclusion in global value chains and the ability to adapt to changes in the external environment.

Digital and cybersecurity research is the additional sphere of the research. Awolowo et al. (2026) emphasize the need for comprehensive cybersecurity assurance of small and medium-sized enterprises through a combination of organizational culture, risk management, and appropriate control mechanisms. Carrapico and Farrand (2024) consider current cybersecurity trends in the European Union within digitalization and geopolitical changes. Hamburg (2023) emphasizes the importance of cybersecurity education and entrepreneur training, which directly links security to the human factor. Koibichuk et al. (2021) demonstrate that the spread of innovative digital technologies is accompanied by new risks of cybercrime and fraud. At the national economy level, the security dimension of digitalization is also associated with the mechanisms of state management of the development of digital technologies in the national security system (Samoilenko et al. (2024)). The study by Krylov et al. (2024) complements this approach by emphasizing the role of innovation infrastructure within digitalization of financial and economic management, while Shaposhnykov et al. (2025) show the relationship between personnel mechanisms and economic security of enterprises.

Digital transformation also depends on the broader institutional, regulatory, and economic environment. The research of regulatory policies and effective public governance demonstrates the importance of institutional conditions for the functioning of economic systems. The influence of institutional factors is also evident through corruption, shadow economy, and tax practices Grosu et al. (2026). The research of the digital economy and sustainable development highlights the need to align technological change with the long-term development goals of Hrubliak et al. (2026), while the development of regional innovation ecosystems is associated with the proliferation of artificial intelligence Popelo et al. (2025) and the interaction of public and private investment in research and development.

Digital transformation also depends on the broader institutional, regulatory, and economic environment. Regulatory policies determine the institutional conditions for the development of digital businesses (Filyppova et al., 2024), and the effectiveness of public administration is an important prerequisite for the functioning of economic systems (Kosach et al., 2022). Bibliometric analysis of regulatory policy confirms a sustained scientific interest in this direction (Zhavoronok et al., 2022). Macrofinancial stability determines the overall environment in which enterprises invest and digital modernization (Nikiforov et al., 2022), while corruption, shadow economy, and tax practices characterize institutional constraints on development (Grosu et al., 2026). At the same time, the digital economy is associated with the tasks of sustainable

development and transformation of economic systems (Hrubliak et al., 2026). At the level of innovation policy, the interaction of public and private R&D investments (Zhang et al., 2025), development of the digital economy and innovation ecosystems (Popelo et al., 2025), as well as state regulation of digital technologies in national security (Rudenko et al., 2024) are important.

Thus, the analysis of modern scientific literature allows us to conclude that the digital transformation of enterprises has at least three interrelated dimensions, including: technological, personnel-organizational, and security (Browder et al. (2024); Han et al. (2025); Li and Wang (2024)). In the biggest part of the studies, these components are analyzed separately: technological digitalization is evaluated through the spread of digital technologies and the transformation of business processes (Kirchmer (2021); Leimstoll et al. (2018)), organizational capacity – through human and intellectual capital, competencies and innovations (Derii et al. (2022); Hryhoruk et al. (2024); Lagodiienko et al. (2025)), and security through cyber risks, protection of digital resources, and the ability to counter threats Awolowo et al. (2026); Carrapico and Farrand (2024); Hamburg (2023); Koibichuk et al. (2021); Samoilenko et al. (2024). Based on the above, the issue of the comprehensive comparative assessment of the transformation of the functioning of business entities, in which technological digitalization, personnel and organizational capacity and digital security are considered as interrelated components of a single system, remains insufficiently studied. It is this research the gap that the comprehensive index of digital transformation of business entities (CIDT) proposed in the paper is designed to fill.

The purpose of the study is to substantiate and evaluate the transformation of the mechanism of functioning of business entities under the impact of digitalization and the changing security environment by determining the digitalization level of enterprises, their personnel and organizational capacity and security readiness, as well as the development of differentiated areas for increasing their adaptability and sustainability.

Methods and Methodology

To achieve the goal of the study, a set of interrelated methods was used, namely: the system method – to substantiate the mechanism of functioning of an economic entity as a set of interrelated technological, personnel, organizational and security components; comparative analysis – to compare the levels of digital transformation of enterprises in the Czech Republic, Hungary, Poland, Romania and Bulgaria; the statistical analysis – to study and generalize initial indicators by country; min-max normalization method – to bring heterogeneous indicators to a single scale 0-1 and ensure their comparability; integral assessment method – to form subindices; weighting method – to calculate the CIDT index; ranking and grouping method – to determine the positions of countries and levels of digital transformation; graphical method – to visualize differences between countries by individual indicators and sub-indices.

To assess the transformation of the mechanism of functioning of business entities, a system of indicators has been chosen, which covers three interrelated dimensions of digital transformation. The first group includes indicators of the digitalization level of enterprises, which characterize the technological basis of changes; the second group includes the hiring of ICT specialists, own and external ICT specialists reflect the personnel and organizational capacity of the enterprises to implement digital changes; the third group – security measures, digital incidents and personnel informing characterize the ability to function safely in the face of digital and external risks. Thus, the selected system of indicators comprehensively covers the chain "technological capabilities → personnel and organizational implementation → safety of digitalized activities", which directly corresponds to the essence of the study of the impact of digitalization and the changing environment on the transformation of the mechanism of functioning of business entities. The indicators were selected on the basis of international standards and the availability of data from Eurostat. Based on the selected indicators, three sub-indices and a comprehensive index of digital transformation (CITT index) were calculated (Table 1).

Table 1. A system of indicators for the digitalization of business operations

Group	Subindex	Indicator	Direction	Reason
1. Digitalization level in enterprises (S1)	$S1=\frac{1}{5}\sum Norm()x$	Companies with at least a basic level of digital intensity (DII)	↑	Direct digitalization level
		Companies that use business software (ERP, CRM, BI) (Business Software)	↑	Depth of digital processes
		Companies that use social media and online advertising (Social Media)	↑	Digital channels
		Companies that have received online orders (at least 1%) (Online orders)	↑	Digital Commerce
		Percentage of companies' revenue from e-commerce (E-commerce share)	↑	Economic impact of digitalization
2. Human Resources and Organizational Transformation (S2)	$S2=\frac{1}{3}\sum Norm()x$	Companies that hire ICT professionals (hiring of ICT professionals)	↑	Workforce Capability
		Companies where ICT functions are performed by in-house staff (in-house ICT professionals)	↑	Internal Competence
		Companies where ICT functions are performed by external providers (external ICT professionals)	↑	Access to External Digital Services
3. The Security Aspect of Digitalization (S3)	$S3=\frac{1}{3}\sum Norm()x$	Companies that implement any ICT security measures (security measures)	↑	Digital Environment Security
		Companies that have experienced any ICT security incidents with consequences (incidents)	↓	The More Incidents, the Worse It Gets
		Companies that inform employees about their ICT security responsibilities (staff training)	↑	Security Culture

Source: Compiled by the authors

In the model, the transformation of the mechanism of functioning of business entities is revealed through three interrelated groups of indicators, which will further form the basis of empirical analysis:

- Group 1 – the digitalization level of enterprises;
- Group 2 – personnel and organizational transformation;
- Group 3 – the security aspect of digitalization.

The Czech Republic, Hungary, Poland, Romania and Bulgaria were selected for the empirical study. The choice of these countries is due to their institutional and regulatory comparability as EU countries of Central and Eastern Europe, the common historical and economic context of the transformation and, at the same time, significant differentiation in terms of the level of digital maturity, human resources and organizational capacity and digital security of enterprises. This configuration of the sample provides the necessary balance between comparability and variability of data and allows to identify different models of transformation of the mechanism of functioning of business entities in a changing external environment.

All primary data were collected for the period 2020–2025.

Each indicator is normalized according to the "minimum-maximum" formula relative to the sample of the studied countries.

For each indicator (i – country, j – indicator): x_{jj}

$$Norm\ () = x_k \left\{ \begin{array}{l} \frac{x_{ij} - min_j}{max_j - min_j}, \text{ if the indicator} \uparrow \\ \frac{max_j - x_{ij}}{max_j - min_j}, \text{ if the indicator} \downarrow \end{array} \right\} \quad (1)$$

Normalized value range: 0-1 (1 is the best result in the sample of countries). An important methodological caveat is that min-max normalization makes the indicators relative to the boundaries of the studied sample. Therefore, the value of the subindex S=1,000 or S≈ 0 does not mean 100% value or absence of this or that indicator, respectively, but characterizes its position relative to the five countries included in the analysis.

Results

It is advisable to consider the functioning of an economic entity as a dynamic process of transforming resources, information and management decisions into economic results under the influence of internal and external factors. In the traditional sense, the mechanism of functioning of an enterprise includes a set of interrelated elements that ensure the formation and use of resource potential, the organization of business processes, managerial decision-making, interaction with counterparties and the achievement of certain economic results.

At the same time, modern economic conditions significantly change the content of this mechanism. The digitalization of the economy, the spread of platform business models, the use of cloud technologies, big data and artificial intelligence, as well as the growth of cyber threats, infrastructure disruptions, logistical restrictions and other security risks form a qualitatively new environment for the functioning of enterprises. Under these conditions, the effectiveness of a business entity is determined not only by the efficiency of the use of resources, but also by its ability to quickly adapt to changes, maintain business continuity, protect digital resources and recover from external shocks.

Therefore, the mechanism of functioning of a business entity is proposed to be defined as a system of interrelated resource, technological, personnel, organizational, managerial and security elements, through the interaction of which the implementation of economic processes, decision-making, creation of economic value, adaptation to changes in the external environment and maintenance of the stability of the enterprise are ensured. To conclude, the digitalization is not a separate direction of enterprise modernization, but a factor in the transformation of the very mechanism of its functioning. At the same time, the security environment is not only an external constraint, since it affects the choice of technologies, labor organization, data management, the formation of reserves, the construction of communication channels and the ability of the enterprise to continue operating under crisis influences.

Modern literature confirms this logic quite well.

Browder et al. (2024) based on two longitudinal case studies showed that digital transformation enhances organizational resilience through the development of five digital capabilities: virtual access, virtual collaboration, data-driven decision-making, algorithmic reprogramming, and supported decision-making.

Awad and Martín-Rojas (2024) explore the relationship between digital transformation and organizational resilience through organizational learning and innovation, which is especially important for the rationale for the HR and organizational transformation group, because digitalization does not create resilience automatically, but is implemented through the organizational capabilities of the enterprise.

Li and Wang (2024), based on data from Chinese companies, showed a statistically significant positive impact of digital transformation on the sustainability of enterprises. The mechanism of this impact is associated with a decrease in agency costs, increased information transparency, and easing of financial constraints. Thus, digitalization changes not only technologies, but also the mechanism of management and resource provision of the enterprise.

Xu et al. (2024a) found that digital transformation increases the resilience of enterprises to supply chain disruptions, and the positive effect is enhanced by diversification of supply sources and geographical diversification, which directly confirms the need to include security and adaptation

aspects in the mechanism of functioning of business entities. At the same time, it is interesting that the results of Wang, Tang, Li (2025) show the nonlinearity of this relationship – a moderate level of digital transformation provides higher corporate resilience, and excessive digitalization does not necessarily give an additional positive effect. That is, not always the more digitalization in the functioning of an entity, the better; the effect of digitalization depends on human resource readiness, organizational capacity, security of the digital environment, and the ability of the enterprise to integrate technology into its own business processes. Another important result was obtained by Xu et al. (2024a): digital transformation has a positive impact on the sustainability of enterprises, and the channels of this influence are green innovation and overall factor productivity.

Thus, most modern works consider the relationship between digital transformation and the adaptability of an economic entity, while the transformation of the mechanism of functioning of an economic entity manifests itself in at least three interrelated planes.

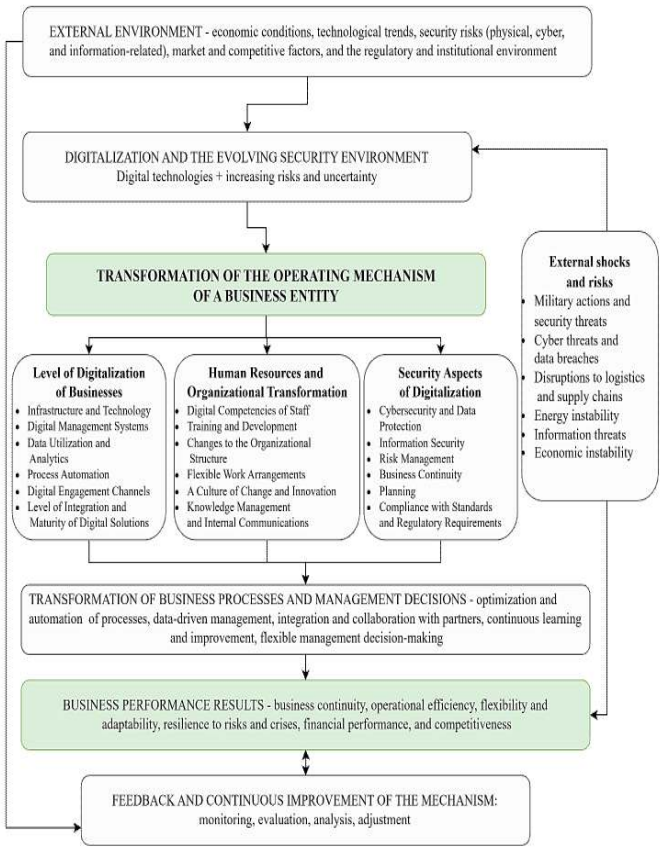
The first is the technological plane, which characterizes the actual digitalization level of the enterprise, covers the spread of digital technologies, the use of cloud services, electronic management systems, digital platforms, data analytics, artificial intelligence and other technological tools. At the same time, digital technologies change not only individual operations, but also the ways of coordinating resources, interacting with customers and suppliers, and making management decisions.

The second is the personnel and organizational plane, since technological transformation is impossible without appropriate changes in human capital and organizational structure. The spread of digital technologies creates the need for new competencies of employees, digital literacy, professional retraining, changes in labor organization models and the development of flexible forms of interaction. Accordingly, digitalization transforms not only the technological base of the enterprise, but also its organizational capacity.

The third is the security plane, which is of particular importance in the context of growing digital and physical risks. An increase in the company's dependence on digital infrastructure simultaneously creates new opportunities and new vulnerabilities. Cyber threats, data leaks, digital infrastructure failures, power outages, disruptions of supply chains, and other external shocks require the integration of security mechanisms directly into the enterprise's operating system.

Thus, digitalization is not an independent technological process, but a systemic factor in the transformation of the mechanism of functioning of a business entity. At the same time, the digital component creates new opportunities, the personnel and organizational component ensures the ability of the enterprise to implement them, the security component determines the conditions for protected operation, and the adaptive-resistant component characterizes the resulting transformation effect (Fig. 1).

Figure 1. Conceptual model of transformation of the mechanism of functioning of an economic entity under the influence of digitalization and changing security environment



Source: built by the authors

The conceptual model reflects the systemic transformation of the mechanism of functioning of an economic entity under the influence of two interrelated groups of factors – digitalization and a changing security environment. Its fundamental feature is the refusal to consider digitalization solely as technological renewal. Digital technologies are considered as a factor in restructuring the ways of organizing activities, resource management, formation of competencies, decision-making and interaction of the enterprise with the external environment.

The initial level of the model is the external environment of the business entity's functioning, which forms a system of opportunities, constraints, risks and covers economic conditions, technological trends, market and competitive factors, regulatory and institutional environment, as well as security threats. In conditions of high uncertainty, it is the external environment that becomes a source of constant need to revise established models of organization of activities. Of particular importance is the changing security environment, which includes physical, cybernetic, informational, infrastructure, energy, logistics, and economic risks. For a modern enterprise, security can no longer be considered as a separate function. The growing dependence on digital infrastructure simultaneously expands the capabilities of the enterprise and creates new vulnerabilities, which necessitates the integration of security components directly into the mechanism of its functioning.

The second initial factor is digitalization, which involves the introduction of digital technologies into business, management, communications, and interaction with stakeholders. Its impact is not limited to the automation of individual operations. Digitalization changes the speed of information exchange, ways of coordinating activities, access to resources and knowledge, the nature of managerial decision-making, and the ability to monitor the external environment.

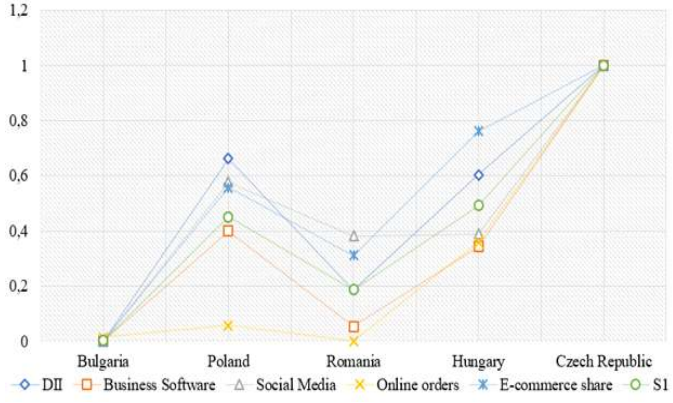
At the intersection of digitalization and a changing security environment, there is a need to transform the mechanism of functioning of an economic entity. It is this block that is central to the proposed model. Transformation does not mean a one-time introduction of certain technologies, but a sequential restructuring of interrelated technological, personnel, organizational, managerial and security elements of the enterprise.

The level of digitalization at enterprises should be interpreted not only through individual indicators, but primarily through the formed sub-index S1, which makes it possible to compare the overall level of digitalization of enterprises in the sample countries (Fig. 2).

According to the results of the normalized indicators, the highest integrated level of digitalization in enterprises was recorded in the Czech Republic – S1=1,000. This means that for all indicators included in the analysis – DII, the use of business software, social networks, online orders, and the share of e-commerce, the Czech Republic has the highest values in the formed sample. At the same time, it is important to note that the value of 1,000 reflects the best position among the countries studied, and not the absolute limit of the digital maturity of enterprises.

The second place is occupied by Hungary (S1=0.491), where the integral digitalization level is almost half that of the Czech Republic. The strongest point of Hungarian enterprises is the share of e-commerce (0.761), while the use of business software (0.343) and social networks (0.389) has significantly lower normalized values. This indicates a certain unevenness of digital transformation, when the development of e-commerce is ahead of the spread of individual internal digital tools.

Figure 2. Average normalized values of indicators of the level of digitalization at enterprises by country and the total value of the S1 sub-index



Source: Eurostat and own calculations

Poland shows a similar result – S1=0.450, occupying the third position. Its advantages are a high level of DII (0.662), active use of social networks (0.576) and a significant share of e-commerce (0.557). On the other hand, the indicator of online orders has a very low normalized value – 0.057, which indicates the heterogeneity of digitalization of various business processes. That is, digital tools are already widely present in the activities of Polish enterprises, but their integration into individual operational processes remains uneven.

For Romania, S1=0.186 was obtained, which indicates a noticeable lag behind the three leaders. The highest among individual indicators is the use of social networks (0.381), while business software (0.053) and online orders (0.000) are characterized by low values. Consequently, the digitalization of Romanian enterprises is more manifested in external digital communication than in deep digital integration of business processes.

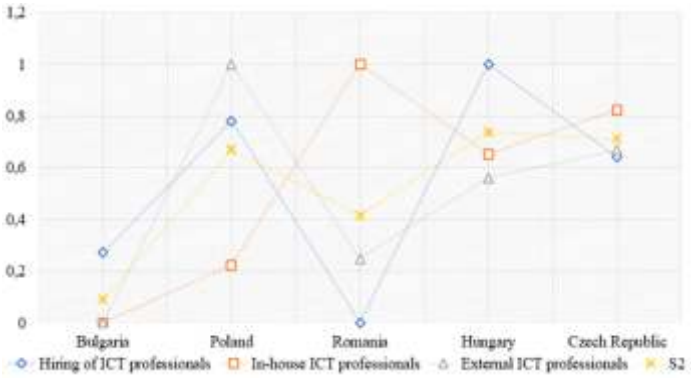
The lowest value of the sub-index was recorded in Bulgaria – S1=0.003. The almost zero values of DII, business software, social networks, and the share of e-commerce indicate the lowest level of digitalization in all the main components of the comparison. At the same time, the indicator of online orders (0.014) also remains close to the minimum.

Thus, there is a significant differentiation of the digitalization level of enterprises between countries. If the Czech Republic forms the upper limit of digital maturity in the studied sample, then Bulgaria is at the opposite pole. Hungary and Poland form an intermediate group with relatively close S1 values, while Romania occupies a lower position.

At the same time, the results show that digitalization in enterprises is multidimensional. High values of one indicator are not necessarily accompanied by similarly high values of others. For example, Hungary has a high position in e-commerce, Poland – in DII and social networks, while Romania demonstrates a relatively stronger result in digital communication, which confirms the feasibility of using the composite sub-index S1, which avoids evaluating digitalization by only one technological parameter.

The level of digitalization itself does not yet determine the ability of an enterprise to function effectively in a changing environment. Therefore, the next step is logically to analyze the indicators of group 2 – personnel and organizational transformation, which will find out how much the technological capacity of enterprises is supported by appropriate human and organizational capabilities (Fig. 3).

Figure 3. Average normalized values of indicators of personnel and organizational transformation by country and the total value of the S2 sub-index



Source: Eurostat and own calculations

The results of normalization of indicators of personnel and organizational transformation demonstrate a noticeable differentiation between countries. The formed sub-index S2 combines three characteristics: the hiring of ICT specialists, the availability of own ICT specialists at enterprises and the use of external ICT specialists. Unlike the first group, these indicators characterize not so much the technological equipment of enterprises as their organizational capacity to provide digital transformation with human and functional resources.

The highest value of the S2 sub-index was recorded in Hungary – 0.738. The country demonstrates the maximum normalized value in terms of hiring ICT specialists – 1,000, as well as high values of the use of in-house ICT specialists in enterprises – 0.652 and external ICT specialists – 0.561. Thus, Hungarian enterprises are characterized by the most pronounced personnel orientation of digital transformation among the countries studied. The combination of internal

competencies with the use of external ICT specialists indicates a combined model of organizational support for digitalization.

The second place is occupied by the Czech Republic – S2=0.711. Its result is the most balanced: all three components are high – hiring ICT specialists (0.640), in-house ICT specialists (0.823) and external ICT specialists (0.669). A particularly high rate of in-house ICT specialists indicates a significant internal organizational capacity of enterprises to support digital processes. Thus, the Czech Republic is characterized by the most balanced structure of personnel and organizational support for digitalization.

Poland received S2=0.668, taking third place. Its strength is the hiring of ICT specialists – 0.780, as well as the extremely high level of use of external ICT specialists – 1,000. At the same time, the value of in-house ICT specialists is only 0.224. This indicates the predominance of a model in which enterprises largely engage external ICT specialists and services, compensating for relatively weaker internal ICT capacity.

For Romania, the S2 value is 0.416. A feature of the country is the maximum value of the indicator of its own ICT specialists (1,000) with the lowest value of the index of hiring ICT specialists. The use of external ICT specialists also remains moderate – 0.248. Thus, the digitalization of Romanian enterprises according to the studied characteristics is more based on the existing internal organizational functions than on the active expansion of ICT personnel or the involvement of external providers.

The lowest result is demonstrated by Bulgaria – S2=0.090. The value of the indicator of own ICT specialists is 0, external ICT specialists – also 0. The hiring of ICT specialists has only 0.271. Thus, Bulgaria is characterized by a significantly lower level of personnel and organizational support for digital transformation compared to other countries in the sample.

Therefore, a high digitalization level of enterprises is accompanied by the same structure of personnel and organizational support. For example, Poland ranks third in the S1 digitalization sub-index (0.450), and in third position in S2, although with a much higher value of 0.668. At the same time, the Czech Republic retains its leading positions both in technological digitalization (S1=1,000) and in personnel and organizational transformation (S2=0.711).

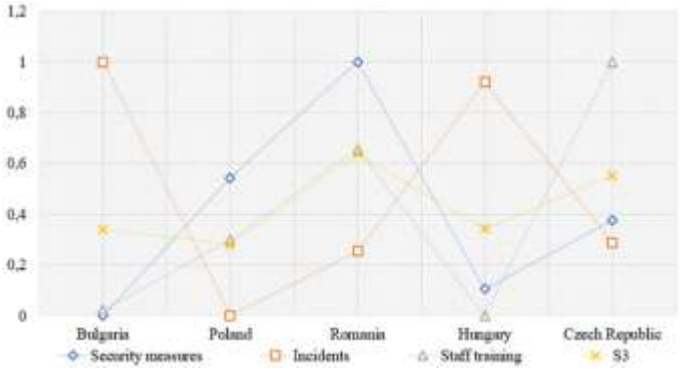
The ratio of Poland and Hungary is especially indicative. Poland has a slightly lower S2, but its model is characterized by a high involvement of external ICT specialists. Hungary, on the contrary, demonstrates the highest intensity of hiring ICT specialists and sufficiently high values of both internal and external ICT specialists. This indicates the existence of different organizational models of digital transformation: internally oriented, externally oriented and combined.

Thus, the results of the analysis of group 2 indicators confirm that personnel and organizational transformation is an independent dimension of digital transformation of enterprises. The availability of digital technologies creates only a potential opportunity to modernize activities, while its actual implementation depends on the ability of the enterprise to provide the necessary ICT competencies, organize relevant functions within the enterprise or effectively attract them from the external environment.

In the context of the proposed conceptual model, this means that S1 characterizes the technological readiness of the enterprise for digital transformation, while S2 characterizes its human and organizational capacity to implement this transformation. It is their combination that creates the prerequisites for the transition to the next dimension – the security of a digitalized enterprise, since the expansion of digital infrastructure and the involvement of internal and external ICT functions simultaneously increases the requirements for data protection, cybersecurity and business continuity.

The third group of indicators characterizes the security aspect of the digitalization of enterprises and reflects the ability of business entities to ensure the protection of digital resources, reduce the likelihood of negative consequences of cyber and information threats, and form an appropriate safety culture among personnel. The group includes three indicators: the prevalence of security measures, the frequency of incidents, and the level of staff awareness of digital security issues. (Fig. 4).

Figure 4. Average normalized values of security indicators by country and the total value of the S3 sub-index



Source: Eurostat and own calculations

The results demonstrate a significant differentiation of countries by the nature of the formation of the security component of digitalization. The highest value of the S3 sub-index was recorded in Romania – 0.637. The country has a maximum normalized value for security measures – 1,000, as well as sufficiently high values for staff information – 0.657 and no incidents – 0.253. Thus, Romania's strength lies primarily in the widespread implementation of formal and technological security measures and sufficient attention to informing employees. At the same time, the relatively low value of the "Incidents" component indicates that the presence of security measures does not completely eliminate the risk of their occurrence.

The Czech Republic ranks second with S3=0.554. Its peculiarity is the maximum result in informing staff – 1,000, which indicates a high level of employee involvement in the digital security system. At the same time, the value of security measures is 0.376, and the incident-adjusted indicator is 0.287. Thus, the Czech security model is characterized by a significant emphasis on the human factor and the formation of a digital security culture.

For Hungary, S3=0.342 it was obtained, it is only slightly inferior to Bulgaria. At the same time, the structure of the sub-index is fundamentally different: the normalized value of the "Incidents" indicator is 0.921, that is, according to this criterion, the country demonstrates one of the best results in the sample. On the other hand, security measures have a value of only 0.105, and staff informing is 0.000. Therefore, a relatively favorable result in terms of the frequency of incidents is not accompanied by similarly high values of preventive measures and staff information.

Bulgaria demonstrates S3=0.341, almost identical to the value of Hungary. Its key advantage is the maximum normalized result for incidents – 1.000. However, security measures have a minimum value of 0.000, and staff informing – only 0.023, which indicates the asymmetric nature of the security profile: a favorable outcome for actual incidents is not supported by an appropriate level of preventive digital security and staff training.

The lowest value of the sub-index was obtained by Poland – S3=0.280. At the same time, the normalized value of safety measures is 0.542, which is a relatively high result, and the information of personnel is 0.299. However, the adjusted incident indicator is 0.000, which significantly reduces the overall value of the sub-index. Thus, there is a certain discrepancy between the availability of security measures and the actual result of incidents at Polish enterprises.

Therefore, the level of digital security of enterprises is not a one-dimensional characteristic. The high prevalence of security measures is not necessarily accompanied by a low frequency of incidents, and a relatively low number of incidents does not necessarily mean a formed system of preventive protection. That is why the simultaneous consideration of security measures, actual incidents and informing personnel allows you to obtain a more comprehensive description of the security environment of enterprises.

The comparison of Romania and Hungary is particularly indicative. Romania has the highest S3 value (0.637) due to the combination of a high level of security measures and staff awareness. Hungary, on the other hand, demonstrates a very high score on the adjusted incident indicator (0.921), but a minimum level of staff awareness (0.000) and a low level of security measures (0.105). Therefore, the same direction of the result for a separate indicator can be formed under fundamentally different models of safety behavior.

The result of the Czech Republic is also indicative, which had a maximum value of S1=1,000 in terms of the

digitalization level of enterprises and at the same time ranks second in terms of the security sub-index S3=0.554. This indicates a relatively coordinated development of the technological and security components of digital transformation. At the same time, the results of Poland show that a high digitalization level does not automatically guarantee a high level of security: for S1, the country ranks third (0.450), while for S3 it ranks last (0.280).

Thus, the results of the analysis of group 3 indicators allow us to draw a fundamental conclusion for the study: digitalization and security are not identical processes. The expansion of the use of digital technologies creates new opportunities for the enterprise, but at the same time increases the importance of protecting information resources, training personnel and managing digital risks. Therefore, a high level of digital maturity should be accompanied by an appropriate development of the security capacity of the enterprise. Within the conceptual model, the S3 sub-index plays the role of a protective component of the transformation of the functioning mechanism. If S1 characterizes technological capacity, and S2 – personnel and organizational capacity, then S3 reflects the ability of the enterprise to protect digitalized processes and ensure their safe functioning.

To summarize the results obtained and determine the complex transformation profile of the mechanism of functioning of business entities, it is advisable to compare the values of the three formed subindices. In contrast to the previous step-by-step analysis of individual indicators, such a comparison makes it possible to determine the structural balance of digital transformation and identify cases when technological, organizational and security components develop with different intensity. The average normalized values of sub-indices before their further weighting are given in Table. 2.

Table 2. Average normalized values sub-indices (before weighting)

Index		Czech Republic	Hungary	Poland	Romania	Bulgaria	Order of countries
Sub-index 1	Digitalization level	1.000	0.491	0.450	0.186	0.003	Czech Republic > Hungary > Poland > Romania > Bulgaria
Sub-index 2	HR & organizational transformation	0.711	0.738	0.668	0.416	0.090	Hungary > Czech Republic > Poland > Romania > Bulgaria
Sub-index 3	Security aspect	0.554	0.342	0.280	0.637	0.341	Romania > Czech Republic > Hungary > Bulgaria > Poland

Source: calculated and grouped by the authors

A comparison of three sub-indices demonstrates that countries are characterized by different profiles of digital transformation, and therefore, their positions cannot be adequately explained only by the general level of technological digitalization.

The most balanced profile is observed in the Czech Republic. The country has a maximum value of S1 and at the same time high values of S2 and S3. The gap in the technological component is not accompanied by a proportional weakening of the personnel, organizational or security components. This gives grounds to characterize the Czech model as one where the digital maturity of enterprises is supported by appropriate internal organizational capabilities and security mechanisms.

Hungary shows a different profile. Its S2 is the highest among all countries, while S1 is in second position and S3 is at the middle level. Thus, the human and organizational capacity of Hungarian enterprises is somewhat ahead of the technological component, which indicates the presence of organizational potential to further deepen digitalization.

Poland is characterized by relatively close values of S1 and S2 – 0.450 and 0.668, respectively, but much lower S3 – 0.280. This configuration is indicative, as it demonstrates the gap between the organizational readiness for digitalization and the security component of its implementation. Therefore, further deepening of digital transformation in such a model requires simultaneous strengthening of digital security mechanisms.

Romania has the most specific profile. For S1, the country is in fourth place, and for S3 – in first place. Thus, a relatively lower level of technological digitalization is accompanied by the highest score in terms of the security component, i.e. safety readiness is not necessarily formed as a derivative of the overall level of digitalization. Enterprises can pay considerable attention to the protection of digital processes even in conditions of relatively less technological maturity.

Bulgaria ranks last for S1 and S2 and fourth for S3. Its profile is characterized not only by a low level of digitalization, but also by an insufficiently formed HR and organizational basis for digital transformation. At the same time, the position for S3 is slightly higher than one would expect given S1 and S2, which also confirms the lack of direct proportionality between technological digitalization and the security component.

Thus, the comparison of sub-indices allows us to distinguish three fundamentally different types of transformation profiles. The first is balanced, represented by the Czech Republic, where the technological, organizational and security components are developed relatively coherently. The second is organizationally oriented, typical for Hungary and Poland, where the personnel and organizational capacity is higher than the technological component. The third is security-oriented, most clearly represented by Romania, where the security component is significantly ahead of the general level of digitalization.

Therefore, the results confirm the absence of a linear relationship between the individual components of the transformation of the mechanism of functioning of enterprises. A high level of digitalization by itself does not guarantee a similar level of organizational readiness or digital security. That is why the further reduction of the three components into an integral assessment should be carried out using reasonable weights, which will determine not only the position of the country in certain areas, but also its overall level of transformation capacity of enterprises.

Based on the average normalized indicators, three sub-indices were calculated. The CIDT index is a comprehensive indicator of the Composite Index of Digital Transformation of the mechanism of functioning of economic entities in the context of digitalization and the changing security environment, taking into account the weighting factors: the level of digitalization at enterprises, personnel and organizational transformation, and the security aspect. A higher value of the CIDT index indicates a better general state of digitalization of the mechanism of functioning of economic entities in the country. The CIDT index includes 3 sub-indices, each of which includes 3-5 indicators:

Index CIDT = S1 * 0.40 + S2 * 0.30 + S3 * 0.30 (2)

where, S1 "Digitalization level of enterprises" – the weight is 40%, since it is digital technologies that are the primary material and technological basis of transformation. The use of digital tools, software, digital channels of interaction and e-commerce directly changes the way business processes, information flows and management decision-making are organized. At the same time, the increased weight of S1 does not mean the dominance of the technological factor over others, but reflects its basic role, without a sufficient level of digitalization, the possibilities of personnel transformation and digital security cannot be fully realized.

S2 "Human Resources and Organizational Transformation" receives a weight of 30%, since digital technologies alone do not ensure the transformation of the enterprise. Their effectiveness depends on the availability of appropriate ICT competencies, the ability to attract specialists, the formation of internal ICT functions and the ability of the enterprise to integrate digital solutions organizationally. Thus, S2 reflects the ability of the enterprise to transform the technological potential into real changes in the mechanism of functioning.

S3 "Security Aspect of Digitalization" has a weight of 30%. The same weight level is due to the fact that in a changing external environment, digitalization simultaneously creates new opportunities and new vulnerabilities. The growing dependence of the enterprise on digital infrastructure, data and information systems increases the importance of cybersecurity, information protection, incident prevention and personnel training. Therefore, security capability is not a supplement to digitalization, but a necessary condition for its sustainable functioning.

For the comprehensive assessment of the transformation of the mechanism of functioning of business entities in the digitalization context and a changing security environment, the aggregation of three formed sub-indices was carried out, taking into account their functional role in the proposed model. Unlike the previous comparison, where each component was considered separately, the Comprehensive Index of Digital Transformation of Business Entities (CIDT) allows you to determine the overall position of the country and at the same time establish which components form its strengths and weaknesses (Table 3).

Table 3. Weighted averages of the sub-indices and the Composite Index of Digital Transformation of Business Entities in the Context of Digitalization and Changing Security Environment (CIDT), 2021–2025

Country	S1 (0,40)	S2 (0,30)	S3 (0,30)	CIDT	Rank	Gradation
The Czech Republic	1,000	0,711	0,554	0,780	1	High level of digital transformation in the face of security challenges
Hungary	0,491	0,738	0,342	0,520	2	Intermediate level (the country has both strengths and weaknesses)
Poland	0,450	0,668	0,280	0,465	3	Intermediate level (the country has both strengths and weaknesses)
Romania	0,186	0,416	0,637	0,383	4	Below average
Bulgaria	0,003	0,090	0,341	0,128	5	Low levels of digital and security maturity

Source: calculated and grouped by the authors

The results of the integral assessment demonstrate a clear differentiation of countries in terms of the ability of enterprises to transform the mechanism of functioning under the influence of digitalization and security challenges. The CIDT value varies from 0.128 in Bulgaria to 0.780 in the Czech Republic, i.e. the gap between the extreme positions is 0.652 points. This indicates a significant unevenness in the digital and organizational and security readiness of enterprises in the studied countries.

The Czech Republic (CIDT=0.780) ranks first and is the only country with a high level of digital transformation. Its advantage lies not only in the maximum S1=1,000, but also in sufficiently high S2=0.711 and S3=0.554. The Czech Republic's result is formed due to the coordinated development of three components. This is fundamentally important. The country not only has a high level of digitalization, but also has human and organizational capacity and a relatively well-established digital security system. For other countries, the Czech profile can be seen as a benchmark for balanced digital transformation, when technological investments are accompanied by the development of human capital and security infrastructure.

Hungary received CIDT=0.520, taking second place. Its peculiarity is the highest value among countries S2=0.738, while S1=0.491 and S3=0.342. The main limitation of digital transformation is not personnel and organizational readiness, but insufficient depth of technological digitalization and security provision. It is advisable for Hungary to direct the existing personnel and organizational potential to accelerate the technological modernization of

enterprises and simultaneously strengthen digital security. The priorities should be the integration of digital technologies into internal business processes, the expansion of the use of modern digital platforms and the strengthening of information security systems. That is, for Hungary, the strategy looks like a strong organizational base → technological deepening → strengthening security.

Poland has a CIDT=0.465 and the third position. Its S2=0.668 significantly exceeds S1=0.450, while S3=0.280 is the lowest among all the countries studied. This is one of the most important results of the study, as it demonstrates the imbalance between the readiness of enterprises for digital transformation and the ability to implement it safely. For Poland, the key reserve for increasing CIDT is not so much building human and organizational capacity, which is already high enough, but strengthening digital security. It is advisable to scale cyber defense systems, increase staff awareness of digital risks, develop incident prevention and response mechanisms. Thus, the strategy looks like this: organizational capacity → secure digitalization → increased resilience.

Romania has a CIDT=0.383 and the fourth position. Its biggest advantage is S3=0.637 – the highest value of the security component in the sample. At the same time, S1=0.186 and S2=0.416 remain low. Romania demonstrates an asymmetric model of digital transformation, in which security readiness is ahead of technological and organizational development of digital technologies. The main task should be to use the already formed security base to accelerate the technological digitalization of enterprises. Particular attention should be paid to digital business processes, e-commerce, software, and the development of ICT competencies. Thus, the strategy looks like this: strong security → acceleration of digitalization → personnel and organizational scaling.

Bulgaria has the lowest CIDT value – 0.128. Unlike other countries, its problem is not concentrated in one separate component. S1=0.003, S2=0.090 and S3=0.341 indicate a systemic deficit in the technological and HR-organizational basis of digital transformation. At the same time, S3 is significantly higher than S1 and S2, that is, even with a low overall digital maturity, a certain security potential has already been formed. Bulgaria needs not a point, but a comprehensive program for the digital transformation of enterprises. Its priorities should be the basic digitalization of business processes, the development of digital competencies, support for small and medium-sized businesses in the acquisition of digital technologies, and the formation of internal ICT functions. The strategy should be: basic digitalization → personnel and organizational support → scaling of security mechanisms.

Thus, the resulting CIDT allows us to move from a simple ranking of countries to the definition of specific directions for digital transformation policies.

Table 4. Differentiated directions for increasing the digital transformation of business entities in a changing security environment according to the results of CIDT

Country	Key Limitation	Priority area
The Czech Republic	the need to maintain balance	Comprehensive deepening of digitalization and sustainability
Hungary	S1 and S3	Technological modernization + digital security
Poland	S3	cybersecurity and digital process protection
Romania	S1 and S2	accelerating digitalization and developing ICT competencies
Bulgaria	S1 and S2	Basic digitalization + frame transformation

Source: calculated and grouped by the authors

That is, increasing the digital maturity of enterprises in a changing environment cannot be provided by a universal set of measures. The results of the CIDT indicate the need for a differentiated transformation policy focused on overcoming the weakest component of the mechanism of functioning of enterprises in each country. At the same time, the results show that technological digitalization, human resources and organizational capacity and security readiness should be considered as interrelated elements of a single mechanism. It is the coordinated development of technological digitalization, human resources and organizational capacity and security readiness that forms a potential basis for increasing the adaptability and resilience of business entities

Discussions

The results of the study make it possible to clarify the understanding of the digital transformation of business entities as a multidimensional process, the effectiveness of which is not determined solely by the scale of the introduction of digital technologies. The proposed CIDT demonstrates that technological digitalization, human resources and organizational capacity and digital security form an interconnected system, but can develop with different intensity. Therefore, the same or close overall level of digital maturity can be formed by fundamentally different combinations of internal capacities. This result is consistent with studies in which digital transformation is considered through digital opportunities, organizational learning, innovation and sustainability of enterprises Awad and Martín-Rojas (2024); Browder et al. (2024); Li and Wang (2024).

This conclusion is consistent with current research that considers digital transformation as a process of developing organizational capacities. Browder et al. (2024) link digital transformation to the formation of digital opportunities that increase organizational resilience, while Awad and Martín-Rojas (2024) emphasize the role of organizational learning and innovation in transforming digital technologies into real organizational outcomes. Li and Wang (2024) also show that digitalization affects not only the technological basis of the enterprise, but also information transparency, agency costs, and financial constraints. Therefore, the results obtained by us support the approach according to which digitalization changes the very mechanism of operation of the enterprise, and not only its technological equipment Kalenyuk et al. (2025); Kirchmer (2021); Leimstoll et al. (2018); Ostrovska et al. (2023).

At the same time, the results allow us to make an important clarification. Maximizing technological digitalization does not necessarily mean maximizing the overall transformative capacity. This is especially important in the context of studies that reveal the non-linear nature of the relationship between digitalization and enterprise sustainability. Wang et al. (2025) show that excessive deepening of digital transformation does not guarantee a proportional increase in corporate resilience. In this context, CIDT complements this discussion: it is not the maximum value of a single digital indicator that is critical, but the consistency of technological, HR, organizational and security capabilities.

It is the difference between the components of the index that is one of the most important results of the study. The Czech Republic demonstrates the highest CIDT (0.780) and at the same time the most balanced combination of S1, S2 and S3. This means that its advantage is not limited to technological digitalization: a high level of technological component is combined with sufficient personnel, organizational and security capacity. This profile corresponds to approaches in which digital maturity is associated not only with technological adoption, but also with organizational capacity and depth of integration of digital solutions (Han et al. (2025); Hryhoruk et al. (2024); Kirchmer (2021)).

At the same time, Hungary and Poland demonstrate why the use of only one generalized digitalization indicator can hide fundamentally different problems. Hungary has the highest value of the HR and organizational component (S2=0.738), but its technological and security components are significantly weaker. Poland, on the other hand, is characterized by a relatively high S2=0.668, but has a low S3=0.280. Therefore, the close positions of these countries

in terms of the overall level of transformation hide a different structure of constraints. For Hungary, the key issue is the conversion of the already formed human and organizational capacity into technological and security strengthening, while for Poland, the elimination of the imbalance between digitalization and security is critical. The importance of the human resources component is consistent with studies on human capital and organizational capacities (Derii et al. (2022); Lagodiienko et al. (2025)), and the importance of the security component – with works on cybersecurity of enterprises (Awolowo et al. (2026); Carrapico and Farrand (2024); Hamburg (2023)).

The profile of Romania is particularly indicative. With the highest among the studied countries S3=0.637, it has a significantly lower level of technological digitalization (S1=0.186). This confirms that digital security is not an automatic derivative of the general level of digitalization. On the contrary, individual components of digital transformation can develop asynchronously. At the same time, this result does not give grounds to assert a causal effect of security capacity on technological digitalization. Rather, it demonstrates the presence of different trajectories of digital maturity formation, which is fundamentally important for benchmarking (Carrapico and Farrand (2024); Koibichuk et al. (2021); Samoilenko et al. (2024)).

Bulgaria is forming a different type of transformational profile – systemically weak in terms of technological and HR-organizational components. S1=0.003 and S2=0.090 determine its lowest CIDT=0.128, although S3=0.341 is markedly higher. This result further confirms that the presence of separate security practices does not compensate for the insufficient technological and organizational base. For such transformational profiles, the formation of basic digital infrastructure, digital competencies, and organizational capacity is of paramount importance (Hrubliak et al. (2026); Krylov et al. (2024)).

Thus, the results of the study allow us to identify four fundamentally different transformation situations: balanced digital transformation; transformation with the dominance of human and organizational capacity; technological and organizational transformation with insufficient security component; and transformation, in which a single security component is ahead of technological development. Such typology is more important than the ranking of countries itself, as it shows how digital maturity is formed, and not only what its aggregate level is. It is also consistent with research on digital maturity, digital business processes, and innovative development (Han et al. (2025); Kalenyuk et al. (2025)).

In this aspect, the proposed CIDT complements existing approaches to assessing digital transformation. Most of the available studies focus either on the level of technological implementation or on the impact of digitalization on individual business outcomes. Instead, the proposed approach makes it possible to simultaneously assess the technological basis of transformation, the ability of personnel and organizations to implement digital changes, and the ability of enterprises to ensure the safe functioning of digitalized processes. That is why it is advisable to consider CIDT not as an alternative to existing digitalization indicators, but as a tool for structural diagnostics of digital transformation (Kalenyuk et al. (2025); Kirchmer (2021); Filyppova et al. (2024)).

An important theoretical implication is also the clarification of the relationship between digitalization and sustainability. Previous research shows a positive link between digital transformation and enterprise resilience, in particular through organizational learning, innovation, productivity, and the ability to respond to supply chain disruptions (Awad and Martín-Rojas (2024); Browder et al. (2024); Li and Wang (2024); Xu et al. (2024a); Xu et al. (2024b)). At the same time, the results of this study show that the potential of digitalization to increase adaptability and resilience depends on the extent to which technological capabilities are supported by organizational and security capabilities. In this context, digital transformation should be considered not as a linear build-up of technologies, but as a process of harmonizing interdependent components of enterprise functioning.

Conclusions

The study made it possible to substantiate that digitalization in a changing external and security environment is not only a technological process, but a complex transformation of the mechanism of functioning of business entities. Its effectiveness is determined by the interaction of technological, personnel-organizational and security components, which was the basis of the proposed conceptual model.

For empirical assessment, three sub-indices were formed: S1 – the digitalization level of enterprises, S2 – personnel and organizational transformation, S3 – the security aspect of digitalization. Their use made it possible to move from assessing individual digital characteristics to a comprehensive comparison of the transformation capacity of enterprises. It has been established that countries have significantly different profiles of digital transformation. High technological indicators are not always accompanied by an appropriate level of organizational readiness or digital security.

For integral assessment, a comprehensive index of digital transformation of business entities in the context of digitalization and a changing security environment (CIDT) is proposed, formed with weights of 40% for S1 and 30% for S2 and S3. This structure reflects the functional logic of the mechanism under study. Digital technologies form its technological basis, the personnel and organizational component ensures the implementation of digital opportunities, and the security component ensures their secure and continuous use. The results of the calculations showed significant cross-country differentiation. The Czech Republic with CIDT=0.780 demonstrated the highest and most balanced level of transformation. Hungary (0.520) and Poland (0.465) formed a group with an average level, but had different internal profiles. Romania (0.383) was characterized by a below-average result with a simultaneously high security component, while Bulgaria (0.128) demonstrated a systemic lag primarily in terms of technological and personnel and organizational components.

The results obtained have a direct practical effect, since CIDT allows not only ranking countries, but also identifying specific areas for improving the mechanism of functioning of enterprises. For the Czech Republic, the priority is to maintain the balance of digital transformation; for Hungary – the use of human resources and organizational potential for technological modernization and security enhancement; for Poland – overcoming the lag in the security component; for Romania – accelerating technological digitalization based on the already formed security capacity; for Bulgaria – comprehensive build-up of basic digital and personnel and organizational capacity.

Thus, the main scientific and practical result of the study is the substantiation of a differentiated approach to the transformation of business entities. Increasing their adaptability and resilience in a changing environment cannot be provided by a universal set of digital solutions, but requires the coordinated development of technological digitalization, human and organizational potential, and digital security, taking into account the specific weaknesses of each country.

A promising area of further research is to check the relationship of CIDT with indicators of adaptability, resilience and performance of business entities, which will empirically establish to what extent the increase in the level of digital transformation really strengthens the ability of enterprises to withstand external shocks, maintain business continuity and adapt to structural changes in the environment.

References

- Awad, J. A. R., & Martín-Rojas, R. (2024). Digital transformation influence on organisational resilience through organisational learning and innovation. Journal of Innovation and Entrepreneurship, 13, 69. https://doi.org/10.1186/s13731-024-00405-4
- Awolowo, I. F., Ode, E., Abidoye, A., Ajao, O., & Jogunola, O. (2026). Cybersecurity assurance for SMEs: A conceptual framework integrating organizational culture, fraud risk management and forensic accounting. Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de l'Administration, e70051.

https://doi.org/10.1002/cjas.70051

- Browder, R. E., Dwyer, S. M., & Koch, H. (2024). Upgrading adaptation: How digital transformation promotes organizational resilience. Strategic Entrepreneurship Journal, 18(1), 128–164. https://doi.org/10.1002/sej.1483
- Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. JCMS: Journal of Common Market Studies, 62, 147–158. https://doi.org/10.1111/jcms.13654
- Derii, Z., Zosymenko, T., Shaposhnykov, K., Tochylina, Y., Krylov, D., & Papaika, O. (2022). The influence of human capital on GDP dynamics: Modeling in the COVID-19 conditions. International Journal of Computer Science and Network Security, 22(3), 67–76. https://doi.org/10.22937/IJCSNS.2022.22.3.10
- Eurostat. (n.d.). Digital economy and society: Database. European Commission. https://ec.europa.eu/eurostat/web/main/data/database
- Filyppova, S., Shaposhnykov, K., Bilousov, O., Seleznova, O., Lozychenko, O. (2024). Regulatory Policy for Development of Digital Business in the National Economy. Pacific Business Review (International), 17(5), 34-42. http://www.pbr.co.in/2024/ 2024_month/November/3.pdf
- Grosu, V., Cosmulese, C. G., Macovei, A. M., Popelo, O., & Zhavoronok, A. (2026). Determining the relationship between corruption, the shadow economy and tax evasion: A comparative econometric analysis in ten European countries. Pacific Business Review (International), 18(8), 113–123. https://www.pbr.co.in/2026/2025_month/February/9.pdf
- Hamburg, I. (2023). Some emerging trends in cybersecurity education and training for entrepreneurs. Proceedings of the International Conference on Business Excellence, 17(1), 971–975. https://doi.org/10.2478/picbe-2023-0088
- Han, Y., Du, H., & Zhao, C. (2025). Development of a digital transformation maturity model for the construction industry. Engineering, Construction and Architectural Management, 32(7), 4384–4412. https://doi.org/10.1108/ECAM-10-2023-1009
- Hrubliak, O., Macovei, A.-G., Hryhorkiv, V., Hryhorkiv, M., & Zhuravel, P. (2026). Synergy of digital economy and sustainable development in a transformation context: EU case for Ukraine. Pacific Business Review International, 18(8), 36–50. https://www.pbr.co.in/2026/2025_month/February/4.pdf
- Hryhoruk, P., Gruzina, I., Greshko, R., Sharko, V., Bohach, Yu., Olyfirenko, I. (2024). The role of intellectual capital in the management of the enterprises' innovative development in the conditions of digitalization. Management theory and Studies for Rural Business and Infrastructure Development, 46(4), 561–569. https://doi.org/10.15544/mts.2024.51
- Kalenyuk, I., Tsymbal, L., & Celika, M. (2025). Digital business transformation: Trends and opportunities in Ukraine. Baltic Journal of Economic Studies, 11(5), 55–64. https://doi.org/10.30525/2256-0742/2025-11-5-55-64
- Kirchmer, M. (2021). Digital transformation of business process governance. In B. Shishkov (Ed.), Business modeling and software design: BMSD 2021 (Lecture Notes in Business Information Processing, Vol. 422). Springer. https://doi.org/10.1007/978-3-030-79976-2_14
- Kochubei, O., Shaposhnykov, K., Grygor, O. , Protsenko, N. , Vyshnevska, O. , Dzyubina, A. (2021). Organizational and Economic Mechanism of Development and Promotion of IT Products in Ukraine. Estudios de economía aplicada, 39(6). https://doi.org/10.25115/eea.v39i6.5264
- Koibichuk, V., Ostrovska, N., Kashiyeva, F., & Kwilinski, A. (2021). Innovation technology and cyber frauds risks of neobanks: Gravity model analysis. Marketing and Management of Innovations, 1, 253–265. https://doi.org/10.21272/mmi.2021.1-19
- Kosach, I., Shaposhnykov, K., Chub, A., Yakushko, I.,

Kotelevets, D., Lozychenko, O. (2022). Regulatory policy in the context of effective public governance: evidence of Eastern European Countries. Cuestiones Políticas, 40(72), 456-473. https://doi.org/10.46398/cuestpol.4072.26

- Krylov, D., Shaposhnykov, K., Shlapak, A., Yakushko, I., Tsyra, O., & Nykoniuk, K. (2026). Development of innovative infrastructure of the national economy under conditions of digitalization of financial and economic system management. Financial and Credit Activity Problems of Theory and Practice, 3(68), 342–356. https://doi.org/10.55643/fcaptp.3.68.2026.5251
- Lagodiienko, V., Shaposhnykov, K., Tanashchuk, K., Shaposhnykova, I., Kakhovska, O., & Stoika, V. (2025). The impact of artificial intelligence and digitization on the educational services market for the protection of human rights and the human capital formation of the national economy. Veredas do Direito, 22, e223466. https://doi.org/ 10.18623/rvd.v22.n2.3466
- Leimstoll, U., Dannecker, A., Knechtli, H., Quade, M., Tanner, C., & Wölfle, R. (2018). E-business in the era of digital transformation. In R. Dornberger (Ed.), Business information systems and technology 4.0 (Studies in Systems, Decision and Control, Vol. 141). Springer. https://doi.org/10.1007/978-3-319-74322-6_6
- Li, C., & Wang, Y. (2024). Digital transformation and enterprise resilience: Enabling or burdening? PLOS ONE, 19(7), e0305615. https://doi.org/10.1371/journal.pone.0305615
- Macovei, A.-G., Burciu, A., Cosmulese, C.G., Shchur, R., Greshko, R., Zhavoronok, A. (2026). The Role of Foreign Direct Investment in the Integration of Romanian Automotive Companies into the Global Value Chain. Financial and Credit Activity Problems of Theory and Practice, 1(66), 444-457. https://doi.org/10.55643/ fcaptp.1.66.2026.5007
- Nikiforov, P., Greshko, R., Marych, M., Marusiak, N., Kharabara, V., Gladchuk, O. (2022). Mutual Influence of Fiscal and Monetary Policy in the Context of Ensuring Macro-Financial Stability of the State. Management Theory and Studies for Rural Business and Infrastructure Development, 45(4), 435-442. DOI: https://doi.org/10.15544/mts.2022.43
- Obydiennova, T., Kharabara, V., Zabashtanskyi, M., Nazarko, S., Havronskyi, A. (2024). The impact of digital transformation on the innovative development of economic systems. Management Theory and Studies for Rural Business and Infrastructure Development, 46(1), 63-70. https://doi.org/10.15544/mts.2024.07
- Ostrovska, N., Krylov, D., Pohrebniak, A., Pereguda, Y., & Stetsiuk, V. (2023). La digitalización como imperativo del desarrollo de procesos empresariales en condiciones de intensificación de la competitividad global. Revista de la Universidad del Zulia, 14(41), 766–783. https://doi.org/10.46925/rdluz.41.43
- Popelo, O., Ivanova, N., Ivanets, S., Perepeliukova, O., Vasyuchenko, P. (2025). Global Trends in Formation of Regional Innovative Entrepreneurial Ecosystems in the Context of Rapid Development of Artificial Intelligence Technologies. Pacific Business Review (International), 18(1), 12-38. https://www.pbr.co.in/2025/2025_month/July/2.pdf
- Rudenko, O., Marhasova, V., Popelo, O., Kosach, I., Sakun, O., Klymenko, T. (2024). Mechanisms of State Management of the Development of Digital Technologies in the National Security System. Revista de la Universidad del Zulia, 15(42), 389-406. https://doi.org/10.46925//rdluz.42.22
- Samoilenko, V., Lagodiienko, V., Pasko, M., Ovod, L., Matsulevych, Ye. (2022). The Mechanism of Labor Motivation as a Determinant of Economic Securityof Enterprises in Competitive Conditions. International Journal of Computer Science and Network Security, 22(2), 385-393. https://doi.org/10.22937/IJCSNS.2022.22.2.49
- Shaposhnykov, K., Filyppova, S., Krylov, D., Ozarko, K., Yudin, M., & Biliaze, O. (2023). Innovative Development of Enterprises in the Context of Digital Transformations of the Institutional Environment of

the National Economy. Management Theory and Studies for Rural Business and Infrastructure Development, 45(3), 233–241. http://dx.doi.org/10.15544/mts.2023.23

- Shlapak, A., Zhavoronok, A., Vdovenko, N., Bilousov, O., Horban, D., Krylov, D. (2025). The Impact of Artificial Intelligence on the Development of the Digital Business Ecosystem. RISUS – Journal on Innovation and Sustainability, 16(2), 180-193. http://doi.org/10.23925/2179-3565.2025v16i2p180-193
- Tanasiichuk, A., Mykhailyshyn, L., Fedoryshyna, L., Lagodiienko, V., Tetyana, R., Polyova, N., & Yurchenko, O. (2024). Strategies for Sustainable Development of Companies in International Markets in the context of Digitalization. European Journal of Sustainable Development, 13(2), 12. https://doi.org/10.14207/ ejsd.2024.v13n2p12
- Wang, Y., Tang, J., & Li, C. (2025). How does digital transformation affect corporate resilience: A moderation perspective study. Applied Economics, 57(2), 121–134. https://doi.org/10.1080/00036846.2024.2350700
- Xu, Y., Jia, F., Wang, L., & Chen, L. (2024). Can digital transformation improve firm resilience to supply chain disruption? Journal of Purchasing and Supply Management, 30(5), 100952. https://doi.org/10.1016/j.pursup.2024.100952
- Xu, Y., Xu, L., Shen, Y., & Fan, Z. (2024). Exploring the effect of digital transformation on firm resilience: Evidence from China. Journal of Asian Economics, 95, 101812. https://doi.org/10.1016/j.asieco.2024.101812
- Yu, W., Zhang, L., Yang, C. (2023). The impact of the digital economy on enterprise innovation behavior: Based on CiteSpace knowledge graph analysis. Frontiers in Psychology, 14. https://doi.org/10.3389/fpsyg.2023.1031294
- Zhang, K., Wang, Z., Yang, Q., Wang, Y. (2025). The changing role between public and private R&D investments in regional innovation: threshold analysis from Guangdong, China. Regional Studies, Regional Science, 12(1), 76–94. https://doi.org/10.1080/21681376.2025.2453573
- Zhavoronok, A., Chub, A., Yakushko, I., Kotelevets, D., Lozychenko, O., Kupchyshyna, O. (2022). Regulatory Policy: Bibliometric Analysis Using the VOSviewer Program. International Journal of Computer Science and Network Security, 22(1), 39-48. https://doi.org/10.22937/IJCSNS.2022.22.1.7
- Zybareva, O., Shylepnytskyi, P., Ozarko, K., Kravchuk, I., & Nahorniuk, O. (2023). The organizational and economic mechanism of attraction of digital technologies in the innovation activity of companies in the conditions of international competition. Revista de la Universidad del Zulia, 14(39), 415-431. http://dx.doi.org/10.46925//rdluz.39.23