

DOI: <https://doi.org/10.34069/AI/2024.74.02.17>

How to Cite:

Melnyk, S., Ravlinko, Z., Shuprudko, N., Pushak, H., & Havrylyshyn, O. (2024). Security aspects of digital transformation and intellectualization of business. *Amazonia Investiga*, 13(74), 201-213. <https://doi.org/10.34069/AI/2024.74.02.17>

Security aspects of digital transformation and intellectualization of business

Aspectos de seguridad de la transformación digital y la intelectualización de los negocios

Received: December 14, 2023

Accepted: January 28, 2024

Written by:


Stepan Melnyk¹ <https://orcid.org/0000-0003-3782-5973>**Zoryana Ravlinko²** <https://orcid.org/0000-0001-8380-6912>**Nataliia Shuprudko³** <https://orcid.org/0000-0002-5629-0671>**Halyna Pushak⁴** <https://orcid.org/0000-0002-2487-8374>**Olena Havrylyshyn⁵** <https://orcid.org/0000-0001-7181-4421>


Abstract


The main purpose of the article is to determine the key aspects of security during digital transformation and intellectualization of business in the conditions of a changing external environment. As a result of the literature review, the team of authors of the article sets themselves a new scientific task, to form an innovative approach to assessing security aspects during digital transformation and intellectualization of business in modern development conditions. The research methodology involves the use of the expert analysis method, the Delphi method, the even comparison method, and the modeling method. Thanks to this, the result was a list of the most significant security aspects affecting the process of digitalization and intellectualization of business in the region. An approach to assessing these aspects has been formed. The innovativeness of the results obtained is considered through the prism of the proposed model for achieving the most important aspects


Resumen


El objetivo principal del artículo es determinar los aspectos clave de la seguridad durante la transformación digital y la intelectualización de las empresas en las condiciones de un entorno externo cambiante. Como resultado de la revisión de la literatura, el equipo de autores del artículo se propone una nueva tarea científica: formar un enfoque innovador para evaluar los aspectos de seguridad durante la transformación digital y la intelectualización de las empresas en las condiciones de desarrollo modernas. La metodología de investigación implica el uso del método de análisis de expertos, el método Delphi, el método de comparación uniforme y el método de modelado. Gracias a esto, se obtuvo un listado de los aspectos de seguridad más significativos que afectan el proceso de digitalización e intelectualización de los negocios en la región. Se ha formado un enfoque para evaluar estos aspectos. El carácter innovador de los resultados obtenidos se considera a través del prisma del modelo

¹ Department of the Finance and Accounting, Lviv State University of Internal Affairs, Lviv, Ukraine.  WoS Researcher ID: AAI-1425-2020

² Doctoral student, Lviv State University of Internal Affairs, Lviv, Ukraine.  WoS Researcher ID: JNH-1737-2023

³ Department of Management, International Economy and Tourism, Chernivtsi Institute of Trade and Economics of Kyiv National University of Trade and Economics, Chernivtsi, Ukraine.  WoS Researcher ID: DRS-2144-2022

⁴ Department of Theoretical and Applied Economics, Lviv Polytechnic National University, Lviv, Ukraine.  WoS Researcher ID: DMV-6663-2022

⁵ Faculty of Publishing, Printing and Informational Technologies, Ukrainian Academy of Printing, Lviv, Ukraine.  WoS Researcher ID: CUZ-1998-2022



of security for effective digitalization and intellectualization of business in Ukraine. The study is limited by taking into account the specifics of the business environment only in Ukraine. Prospects for further research suggest expanding the range of modeling; if only the IDEF0 method was used in the article, then in the future the possibilities of using IDEF3 should be considered.

Keywords: business, security, digital transformation, business environment, intellectualization.

Introduction

Digital transformation within the framework of the functioning of each individual enterprise has become relevant relatively recently, but today it is already the main condition for maintaining competitive advantages and creating the necessary digital foundation for development in the context of an increasing share of the digital economy. COVID-19 became an indicator that determined significant benefits for businesses that were able to operate online. The post-pandemic period has not diminished, but increased, attention to a holistic vision of the prospects for introducing digital technologies with a rethinking and restructuring of all business processes. The difference in the development of the national economy, manifested in the readiness of the digital infrastructure for business activity in matters of digital transformation, determines different initial positions with the benefits of enterprises operating in economically developed countries. Ukraine lags behind its EU neighbors in economic development, and military actions have provoked a significant number of refugees, which has caused personnel losses that are slowing down the digital transformation of Ukrainian enterprises. A thorough study of the best practices of digital transformation of enterprises in the EU countries in comparison with the actual circumstances of such processes in Ukraine creates the necessary information basis for predicting changes in the struggle for competitive positions in the domestic and foreign markets, in particular in terms of eliminating threats and better using new opportunities arising through displacement of significant numbers of highly skilled and motivated refugee workers.

The passivity of Ukrainian enterprises regarding digital transformation and intellectualization on an individual basis is fraught with the loss of competitive positions due to the inability to meet

propuesto para lograr los aspectos más importantes de seguridad para una digitalización e intelectualización efectiva de las empresas en Ucrania. El estudio se limita a tener en cuenta las características específicas del entorno empresarial únicamente en Ucrania. Las perspectivas de futuras investigaciones sugieren ampliar la gama de modelos; Si en el artículo solo se utilizó el método IDEF0, en el futuro se deberían considerar las posibilidades de utilizar IDEF3.

Palabras clave: negocios, seguridad, transformación digital, entorno empresarial, intelectualización.

consumer needs at a higher technological level, and within the national economy - a deepening of the technical and technological gap with an increased orientation towards raw materials and labor exports and a decrease in purchases. Consequently, the issue of digital transformation and intellectualization of enterprises is especially acute due to the growing uncertainty of the external environment, which requires, in order to maintain competitiveness, the transformation of activities through the introduction of modern information technologies and digital management tools, ensuring digital shifts. If in economically developed countries this is a matter of strategic and tactical perspective of operation, illustrated by the ability to maintain the active activity of enterprises during restrictions during the COVID-19 period, then for Ukraine it is a matter of its own survival, restoration of macroeconomic balance and laying the resource foundation for post-war recovery and the ability to technologically follow for the leading countries in economic development.

The main purpose of the article is to determine the key aspects of security during digital transformation and intellectualization of business in the conditions of a changing external environment.

Literature review

The transition to digital platforms and the intellectualization of business, especially in a fluctuating external environment, presents multifaceted challenges and opportunities, as explored in a range of scholarly works.

Thus, in the study by Javaria et al. (2020) focuses on identifying and managing the risks consumers face as e-commerce evolves. In the context of your topic, this resource provides insights on the

security aspects associated with digital transformation in e-commerce and points to strategies that can help mitigate these risks. Coverage of methods for identifying and countering potential threats is important to maintaining consumer safety in a changing environment. While Javaria et al. (2020) discuss identifying and managing risks in e-commerce, they primarily focus on the consumer side of security. Our article appears to adopt a broader organizational perspective, emphasizing the security aspects affecting the overall business process during digital transformation, rather than just consumer interaction. Our innovative assessment model offers a holistic view that encompasses the entire business environment.

Alazzam et al. (2020) offer insights into the legal intricacies of electronic commerce, highlighting the obstacles and solutions within Jordanian and comparative legislatures, crucial for understanding the legal framework surrounding digital business transactions. This is complemented by Zybareva et al. (2022) investigation into the management of business projects, emphasizing the role of international competitiveness in global sustainability conditions. Their perspective is crucial in understanding how businesses can adapt and thrive in an increasingly interconnected world.

In a study by Kopytko et al. (2023) the authors propose a methodology for optimizing financial resources in order to increase the level of economic security of enterprises in a dynamic external environment. In the context of our study, this clearly understands the importance of financial stability and economic security in the context of digital transformation and business intelligence, as well as for developing strategies to optimize resources. Kopytko et al. (2023) propose methods for optimizing financial resources to enhance economic security, focusing specifically on financial strategies. Our methodology, which includes expert analysis, the Delphi method, and even comparison, allows for a more comprehensive approach to assessing security in the context of digital transformation, beyond just economic security.

The development of e-commerce platforms, as discussed by Alazzam et al. (2023), brings to light the importance of information models in modern socio-economic systems. Their research underscores the need for legal compliance and global digitalization, providing a framework for the successful integration of e-commerce in business operations. Similarly, Lagodiienko et al. (2022) examine the management of foreign

economic activities in sustainable conditions, offering insights into how enterprises can navigate the international market amidst sustainability challenges.

The work of Fischer et al. (2020) illuminates the archetypes of digital transformation strategies using business process management to define meta-goals. This article can serve as a source of information about different approaches to digital transformation and their impact on business processes. This will provide a better understanding of how strategic planning and management can facilitate successful adaptation to changes in the external environment.

At the same time, Zhou et al. (2021) analyzes the impact of enterprise intellectualization on its leadership potential. In the context of your topic, this resource is important for understanding how the integration of intelligent systems and processes can enhance business competitiveness and leadership in a changing environment. The importance of an innovative approach to leadership and strategic development is highlighted. Zybareva et al. (2021) bring attention to the economic and legal aspects of network readiness of enterprises in Ukraine, offering a perspective on how businesses can improve through digital and network enhancements. This is particularly relevant in understanding the legal ramifications and economic strategies needed for digital transition. Studies like that of Zybareva et al. (2022) and Lagodiienko et al. (2022) address global sustainability and international market navigation, but they might not integrate these factors with digital transformation security. Our innovative model could be seen as integrating these concerns by providing a security assessment that considers digital transformation as a factor contributing to international competitiveness and sustainability.

Kim et al. (2021) explores the essence, characteristics and consequences of modern digital transformation. It can provide your research with a deeper understanding of where the digital era is heading and the challenges and opportunities it poses for businesses. Analyzing the future direction of digital technologies and their impact on business models, management and competitiveness is key to adapting to changing environmental conditions.

The study by Trokhymets (2020) examines the development of the national economy in the context of information processes and digitalization. The author analyzes how digital technologies and information systems influence

economic structures and processes at different levels: global, national and regional. In the context of our topic, this source can provide valuable insight into the impact of digital transformation on the economy, which in turn highlights the importance of security aspects in the process of integrating emerging technologies. A focus on national economic development helps understand macroeconomic trends and the challenges businesses face as they adapt to digital innovation, highlighting the need to ensure digital security at all levels. In conclusion, Sylkin et al. (2021) effectively highlight the critical need for businesses to adapt their economic security management in response to the rapid digital transformation and intellectualization of business practices sparked by the global pandemic. This work serves as a valuable resource for those looking to understand the security imperatives in the digital age, providing both theoretical insights and practical guidance for navigating the complex landscape of modern business operations.

Shtangret., Korogod., Bilous., Hoi, & Ratushniak (2021) focus on the management of economic security in the high-tech sector, emphasizing the necessity of modernizing security practices to cope with the dynamic threats emerging from rapid technological advancements. Their study highlights the urgency of integrating sophisticated security management tools and techniques to protect critical infrastructures and sensitive data against cyber threats exacerbated by increased digital dependency. Dubyna et al. (2023) extend this discussion to the trading

sector, analyzing how digitalization serves as both a tool and a challenge for maintaining financial and economic security under external shocks, such as global health crises or economic instability. Their research underlines the dual role of digital technologies that offer innovative solutions for robust security mechanisms while simultaneously presenting new vulnerabilities that must be managed carefully. The findings suggest that proactive management of digital resources and continuous adaptation of security strategies are essential to safeguard trading enterprises from the volatile external environment. Both studies stress the importance of a methodological approach to security in the digital era. Sylkin et al. (2020) contribute to this body of knowledge by developing a model for assessing financial security levels that businesses can use to quantify and manage their security postures effectively. Their methodology allows organizations to systematically evaluate their financial vulnerabilities and prepare more comprehensive defense mechanisms against potential threats. This model is particularly relevant in contexts where businesses are seeking to balance growth and security in an increasingly interconnected and digitalized market landscape.

Collectively, these studies provide a multi-dimensional understanding of the challenges and strategies in the digital transformation and intellectualization of businesses, offering valuable insights into the legal, economic, and strategic aspects in a rapidly changing external environment. But along with this there are a number of gaps in the literature (Table 1).

Table 1.
Key gaps in the literature on the topic of the article

Gaps	Characteristics
The proposed approach	Lack of a modern methodical approach to security modeling
Consideration of security	In the literature when considering the digitalization of business, there is no issue of ensuring security
The issue of intellectualization	The intellectualization of business is rarely the focus of the literature

Source: (formed by authors)

As a result of the literature review, the team of authors of the article sets themselves a new scientific task, to form an innovative approach to assessing security aspects during digital transformation and intellectualization of business in modern development conditions.

Methodology

Expert analysis and the Delphi method formed the cornerstone of your approach, providing a

robust framework for identifying critical security aspects. By engaging a panel of experts and employing a systematic, iterative process of surveys, the study harnessed collective intelligence and expert insights. This methodology is particularly effective in reaching a consensus on complex issues where individual understanding may be limited or highly variable. It ensured that the security aspects identified were not only comprehensive but also reflective of current industry and academic perspectives.

To prioritize and compare these identified security aspects, the pairwise comparison method was adopted. This method is particularly useful for its simplicity and effectiveness in breaking down complex decisions into a series of simpler comparisons. It enabled a systematic evaluation of each security aspect against the others, ensuring that the most critical aspects were highlighted based on consistent and logical comparisons. This approach is instrumental in distilling a range of potential security concerns down to the most pivotal ones.

30 experts from the leading areas of business security were involved in order for them to help establish 5 key aspects of the security of digitalization and intellectualization of business in Ukraine. Since there are many experts themselves, they were forced to use the Delphi method to organize them. Next, the final list agreed through mathematical modeling programs is highlighted, the key results are highlighted. Following the identification of these critical aspects through the Delphi method, the study employed the pairwise comparison method to

prioritize and systematically evaluate these aspects against each other. This method simplified the complex decision-making process by breaking it down into smaller, more manageable comparisons. Each security aspect was compared with every other to establish its relative importance or urgency.

Finally, the IDEF0 method was leveraged for modeling the effective implementation of these critical security aspects in Ukrainian businesses. IDEF0 is a functional modeling methodology used for the analysis, development, reengineering, and integration of information systems, business processes, and software engineering. This method provided a structured framework for conceptualizing how the identified security aspects could be effectively integrated into business processes. By using IDEF0, your study not only identified key security aspects but also mapped out a clear, actionable path for businesses to enhance their security in the face of digital transformation and intellectualization (Fig.1).

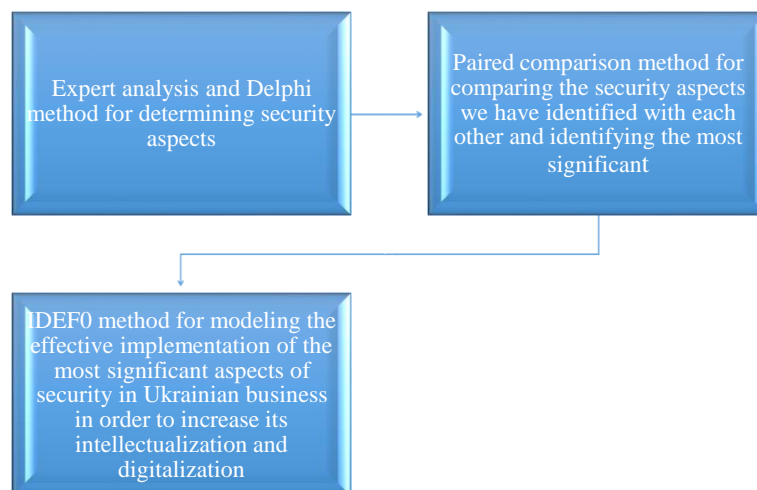


Figure 1. The main methods used in the article. Source: (formed by authors)

The application of IDEF0 began with the identification and decomposition of primary business functions into simpler, manageable sub-functions. This breakdown facilitated a detailed examination of where and how security vulnerabilities could arise as businesses digitalized and intellectualized their operations. Each sub-function was then assessed to determine specific security needs, ensuring that all potential threats were accounted for systematically. Building on this foundation, the study used the IDEF0 diagrams to map out the interactions between these functions and their

respective security requirements, effectively creating a visual and logical representation of workflows and data flows.

Together, these methodologies provided a comprehensive, multi-faceted approach to understanding and addressing the security challenges inherent in the digital and intellectual evolution of businesses in an ever-changing external environment.

Results and discussion

In the EU countries, three levels of digital maturity of enterprises can be identified: the first, where investment is made in individual digital technologies, the application of which does not have a significant impact on the overall activity, but is an embodiment of the desire to follow competitors in the position that provided certain competitive advantages; the second – the gained experience allows forming a portfolio of digital solutions, within which the necessary investment volumes, risks, expected effect, and the degree of impact on the overall financial results of the activity are assessed; the third – a developed strategy serves as the basis for systematic updating of the list of relevant digital technologies, which ensures strengthening of competitive positions due to leadership and maximum readiness to operate in the conditions of the digital economy.

The necessity to pay due attention to the digital transformation of enterprises in Ukraine is conditioned by the business's realization of the global nature of this issue, which requires resolution. By 2022, i.e., in a period when military actions were not the main threat to the functioning of Ukrainian enterprises, 90% of enterprises passive to the implementation of digital technologies felt an increase in competition from those that had made real steps in the digitization of business processes. In terms of digital transformation of enterprises by scale of activity, the most complex situation was in large industrial enterprises, 95% of which were passive to the widespread introduction of digital technologies, continuing to rely on technological processes created sometimes 30 years ago for the production of technologically simple, material- and energy-intensive products for domestic consumers. At the same time, the management of 71% of these large enterprises noted an

intensification of competition with a high probability of losing competitive positions in the short term.

Information from the survey of management of Ukrainian enterprises is almost fully confirmed by analytical data from the State Statistics Service of Ukraine. Such research has been conducted since 2018 and actually contains diverse information due to the constant clarification of the research object, but despite this, it provides a general idea of the intensity of use of digital technologies before and during military actions. According to these official statistical data, the share of enterprises that had access to the Internet virtually did not change (2018 – 88.0%, 2019 – 86.4%, 2021 – 86.6%, 2022 – 85.1%) and was insufficiently high, as in the conditions of the digital economy without information exchange, there is practically no possibility to conduct business, and here more than 10% of operating enterprises were deprived of such an opportunity. Equally interesting are the details of access to the Internet, as significantly fewer enterprises had fixed access, i.e., in 2018 – 62.1%, 2019 – 60.9%, and in 2021 – 61.8%. Another quality indicator – Internet speed – shows that in 2021, 18.2% of enterprises used connections with speeds less than 30 Mbps and another 21.8% – from 30 Mbps to 100 Mbps. Collectively, such data indicate limitations in Internet access and low quality of using this data transmission tool, as well as insufficient development of digital infrastructure, which has already been emphasized above.

One of the traditional and most actively used tools of digital marketing remains the website. According to analytical data, the share of Ukrainian enterprises using such a tool was critically low: 2018 – 35.7%, 2019 – 35.2%, and 2021 – 35.3%." However, anything related to security must be referred to as "security.

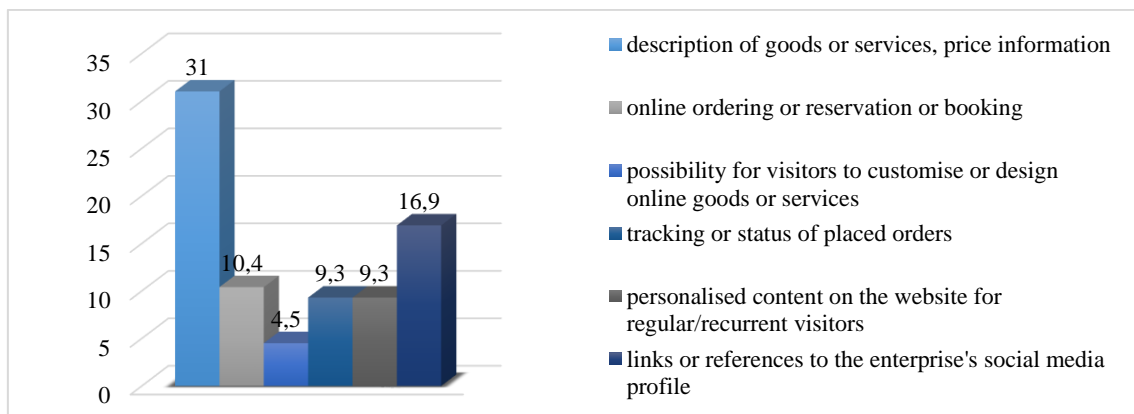


Figure 2. Functional capabilities of the website of enterprises in Ukraine in 2022. (formed by authors)

An even more complex situation arose in 2021 regarding: the use of chat services for customer communication, which was relevant for only 9.1% of enterprises; the purchase of cloud computing services was applied by 10.2% of enterprises; additional hiring of IT professionals was conducted by 22.3% of enterprises; and the production of products using robotics occurred in just 2.9% of enterprises. Collectively, these data indicate both a critically low level of digital technology usage and the technological backwardness of Ukrainian enterprises compared to competitors from economically developed countries, depriving them of competitive advantages both in the domestic market and limiting their effectiveness in global markets.

One of the specific characteristics of digital transformation in enterprises is the need for continuous technological updating, which is possible in the case of improving the digital competencies of employees. Analytical data provide a general idea of the intensity of knowledge improvement by ICT specialists and other employees involved in enterprises: 3.7% and 4.1% in 2018; 3.8% and 4.3% in 2019; 4.5% and 4.4% in 2020. We will further emphasize the importance of intellectualization, and these data serve as an informational basis that this issue will be very acute, as previously necessary attention was not paid to improving the professional and digital competencies of employees.

Security aspects of implementing digital transformation consist not only in the ability to establish a corresponding list of challenges, risks, and threats that will be relevant for a particular enterprise, but also in considering the fact of the duration, and actually the continuity of changes, which largely concern management and personnel. This involves two important points: firstly, the need to prevent and eliminate internal corporate resistance; secondly, stimulating the acquisition of new professional and digital skills. The first point is related to the typical behavior of each individual, i.e., the desire to maintain consistency in the way of life and work activity, as any change provokes the need for adaptation and adjustments, which is accompanied by disturbance, additional psychological and physical loads, etc. The reluctance to change, especially in the absence of understanding of the process and possible consequences, causes resistance, which can be manifested in the form of a passive attitude towards the execution of tasks and participation in digital transformation, or even deliberate actions with a distinctly hostile character. Such aspects are real, considering that in the program of digital transformation of the

enterprise, typical measures include automation and robotization, which provoke a reduction in the necessary workforce, and thus pose a threat of job loss for individual employees, and may lead to disturbances in the moral-psychological climate in the collective with an increase in the number of conflict situations, a decrease in discipline, an increase in cases of resignations due to the inability to continue active work activity, and a decrease in labor productivity. Countering such a negative course of events, which threatens both the failure to achieve the goals of digital transformation and significant losses due to incurred costs for implementing the program, requires the activation of security activities, particularly based on conducting explanatory work, which should involve informing every executor of the enterprise's digital transformation of the justification of the necessity of changes, his tasks, strategic guidelines in general, and the advantages that he will personally receive. The key emphasis should be on the fact that such changes are made based on the possibility of joint achievement of the interests of owners, management, and employees. Successful practice in reducing resistance involves engaging all employees, regardless of their level of participation in the enterprise's digital transformation process, in transparent communication, exchange of opinions, consideration of positions, and providing the opportunity to show initiative that corresponds to the content of the planned measures.

We have 5 key aspects of the security of digitalization and intellectualization of business in Ukraine:

A1. Data protection. Ensuring data confidentiality, integrity and availability is critical. This includes protection against unauthorized access, data loss, as well as ensuring data backup and recovery after possible incidents.

A2. Cybersecurity. Protection against cyber threats such as viruses, malware, phishing, and other types of cyber attacks. It is important to have modern antivirus solutions, firewalls, and intrusion detection and prevention systems.

A3. Compliance with regulatory requirements. It is important to consider local and international legislation related to digital activities, including requirements for the protection of personal data.

A4. Physical security. Ensuring physical protection of the infrastructure used for digitalization (servers, network equipment, etc.).

This includes access control, CCTV systems, anti-terrorism measures, etc.

A5. Education and training of personnel. Raising awareness and training of employees in the field of cybersecurity and proper handling of data. This helps prevent accidental or unintentional information leaks.

To perform a detailed Analytic Hierarchy Process (AHP) analysis and create a reachability and dependency matrix for the five key aspects of digitalization and intellectualization of business security in Ukraine, we need to follow several steps:

1. Create Pairwise Comparison Matrices. Based on expert opinions, two matrices will be created. Each aspect will be compared with every other aspect, and their relative importance will be assigned values.
2. Calculate Weights and Consistency Indicators. For each matrix, we'll calculate the weights (or priorities) of each aspect and the consistency ratio to ensure the judgments are reliable.
3. Create Reachability Matrix. This matrix will identify which aspects can reach or influence other aspects.
4. Create Dependency Matrix. This matrix will show how dependent each aspect is on the others.

Lets creat Pairwise Comparison Matrices (Table 2).

Table 2.
Pairwise Comparison Matrix

	A1	A2	A3	A4	A5
A1	1	2	3	4	5
A2	1/2	1	2	3	4
A3	1/3	1/2	1	2	3
A4	1/4	1/3	1/2	1	2
A5	1/5	1/4	1/3	1/2	1

Source: (formed by authors)

Each element in the pairwise comparison matrix is divided by the sum of its column. This normalization process turns the original matrix into a matrix where each column sums up to 1. The average of each row of the normalized matrix is calculated. These averages represent the weights or priorities of each aspect.

Multiply the original matrix by the weights vector. Divide each element of this product by

the corresponding element in the weights vector. Calculate the average of these quotients to find the maximum eigenvalue (λ_{max}).

Let's calculate these values using our matrix. We will illustrate the calculations for normalizing the matrix, calculating the weights, and then finding the maximum eigenvalue, CI, and CR. Normalized matrix is in Table 3.

Table 3.
Pairwise Comparison Matrix

	A1	A2	A3	A4	A5
A1	0.43	0.49	0.43	0.38	0.33
A2	0.21	0.24	0.29	0.28	0.26
A3	0.14	0.12	0.14	0.19	0.2
A4	0.109	0.08	0.07	0.096	0.13
A5	0.088	0.06	0.049	0.04	0.067

Source: (formed by authors)

The weights are calculated as the average of each row in the normalized matrix.

- A1. Data Protection: 0.416
- A2. Cybersecurity: 0.262
- A3. Regulatory Compliance: 0.161
- A4. Physical Security: 0.099

A5. Personnel Education & Training: 0.062.
Calculated as the average of the quotients of the weighted sum vector by the weights vector. λ_{max} : 5.0683.

CI: 0.0171.
CR: 0.0153.

So, its mean that A2 is most value security aspect for digitalization and intellectualization of business in Ukraine. Lest buld IDEF0 model to

improve it. To begin with, the node tree of the model blocks (Fig. 2).

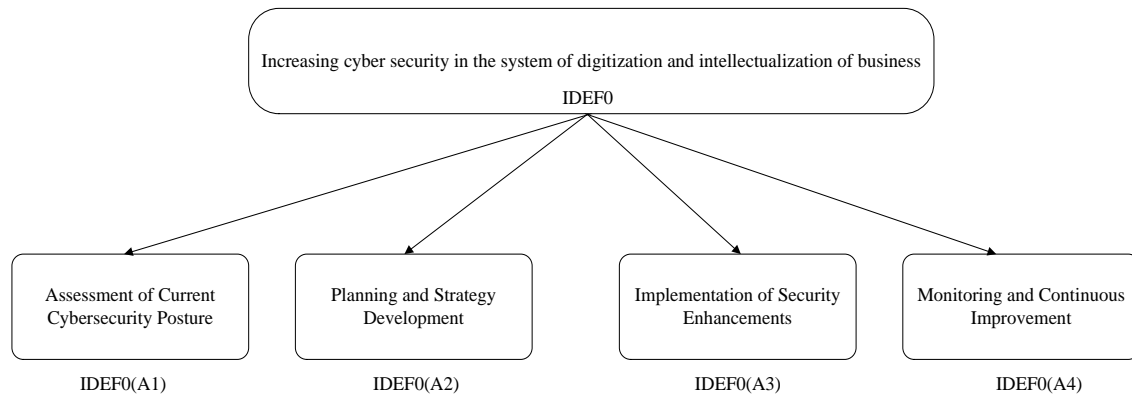


Figure 3. The node tree of the model blocks.
Source: (formed by authors)

To develop an effective IDEF0 model for enhancing cybersecurity, we can break down the process into four main stages:

A1. Assessment of Current Cybersecurity Posture. Evaluate the current state of cybersecurity measures in the organization. This includes assessing existing security policies, network infrastructure, software, hardware, and employee awareness levels.

Inputs: Current cybersecurity policies, network architecture diagrams, software and hardware inventory, employee survey data.

Outputs: Comprehensive assessment report detailing vulnerabilities, strengths, and areas for improvement.

A2. Planning and Strategy Development. Based on the assessment, develop a strategic plan to address identified cybersecurity weaknesses. This includes updating or creating new security policies, identifying necessary technological upgrades, and planning training programs for employees.

Inputs: Assessment report, industry best practices, budgetary constraints.

Outputs: Cybersecurity improvement plan, updated security policies, training schedule, technology upgrade list.

A3. Implementation of Security Enhancements. Execute the cybersecurity improvement plan. Implement new security technologies, update systems, and conduct employee training sessions. Ensure that all changes are in compliance with local and international cybersecurity regulations.

Inputs: Cybersecurity improvement plan, updated security technologies, training materials.

Outputs: Enhanced cybersecurity infrastructure, trained workforce, compliance documentation.

A4. Monitoring and Continuous Improvement. Regularly monitor the cybersecurity measures to ensure their effectiveness. This includes continuous threat assessment, periodic reviews of security policies, and incorporating feedback from employees. Stay updated with the latest cybersecurity trends and threats.

Inputs: Security monitoring tools, employee feedback, industry updates.

Outputs: Monitoring reports, updated security policies, feedback implementation plan (Fig.3).

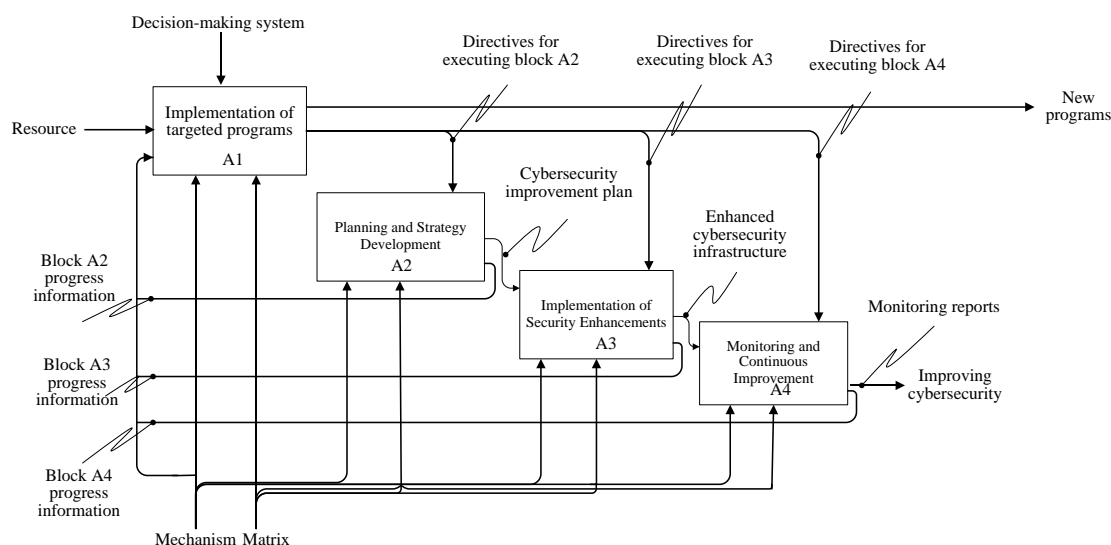


Figure 4. The main IDEF0 model to increasing cyber security in the system of digitization and intellectualization of business.

Source: (formed by authors)

Each of these stages should be detailed in the IDEF0 model with clear connections, indicating how the output of one stage becomes the input of the next. This systematic approach ensures a comprehensive strategy for enhancing cybersecurity in the context of business digitalization and intellectualization in Ukraine.

Discussing the results obtained, it should be noted that a critical analysis of the conditions and actual activity of the digital transformation of enterprises in Ukraine, in particular based on the significant impact of military operations and the prospects for post-war economic recovery, clearly demonstrated the following points:

- the processes of digital transformation are objective, they are occurring and will continue to occur regardless of the activity of individual business entities under the pressure of the changes that are taking place in the global economy as a whole;
- maintaining competitiveness requires searching for financial resources for technical and technological renewal and searching for the optimal option for using digital technologies;
- the process of digital transformation is indefinite, which provokes systematic changes with a violation of constancy in functioning, and therefore the need for activities and temporary stabilization of the situation;
- the problem of the effectiveness of digital transformation is determined by the motivation and intellectual level of management and employees, which, in the

context of the loss of human resources due to a significant number of refugees in the EU countries and internally displaced persons, requires due attention to issues of intellectualization;

- each enterprise forms and implements its own digital transformation program, which must be balanced, take into account the current state of the enterprise, changes in the national economy and the expansion of the boundaries of the digital economy in the global economic space.

Expanding business access to digital technologies has become the basis for the emergence of new business models, when previously existing forms of business organization are forced to be modernized in order to maintain competitive advantages and adapt to the conditions of increasing the share of the digital economy within the traditional one. Such processes exist in every national economy, but occur with varying intensity due to digital transformation at the macro level, which is determined by the level of development of digital infrastructure. In Ukraine, as a country lagging behind the EU countries in economic development, an increase in the share of the digital economy, on the one hand, increases threats to enterprises that maintain established business models and are passive in the introduction of digital technologies, but on the other hand, creates new opportunities for improving competitiveness through the formation of competitive advantages, which resonates with consumers. Conventional digitization cannot ensure the preservation of

competitive positions, nor can fragmented investment in digital technologies. The priority is to rethink holistic guidelines, where digital technologies act only as tools, the effectiveness of which depends on the intellectual level of the performers, that is, management and employees. The starting point should be an understanding of the goals that must be achieved based on the digital transformation of the economy, the selection of digital technologies that ensure the achievement of such goals, the creation of a map for the implementation of transformations in the key of changing business processes and the transition to a new business model, while not leaving without attention issues of financing innovations, the possible emergence of threats and the expected effect, that is, a strategy for the digital transformation of the enterprise must be developed. The priorities of such a strategy should be: creativity in contact with consumers, non-linearity of the management hierarchical structure, individuality in the production of products with a reduction in the chains of intermediaries, high speed of changes in business processes together form the basis for implementing digital transformation at the level of individual enterprises. Security aspects are important, which lie in the fact that digital transformation in an enterprise represents a certain radical technological revolution, when loss of control threatens the cessation of activity. That is, in fact, there are two extremes: passivity - leads to the loss of competitive positions with subsequent liquidation; digital transformation in the absence of strategic vision and control over the process also does not guarantee an exclusively positive result. Consequently, such radical changes, driven by an increase in the share of the digital economy, require a targeted and balanced approach. Military actions burden such a process, but also create additional advantages for those enterprises that are moving towards the goal, ahead of competitors.

For example, Schwarcz (2023) delves into the evolving nature of commercial law in the digital age. Schwarcz's insights into the flexibility and adaptability required in commercial law offer a parallel to our study's focus on the dynamic nature of digital transformation and the need for innovative security approaches.

A study by Sylkin et al. (2018) focuses on assessing the financial security of engineering enterprises, considering it a critical condition for the application of crisis management. It emphasizes the practical aspect of identifying and addressing financial risks to prevent business crises. Our research, on the other hand, has a

broader focus as it covers digital transformation and business intelligence, with an emphasis on security aspects in a dynamic external environment. Our approach involves developing an innovative methodology for assessing security that differs from a direct focus on financial stability at work.

Ferrari (2022) investigates non-technological factors in family businesses, highlighting the importance of considering various elements, including security aspects, in the digitization of business processes. This perspective complements our research by underscoring the multifaceted nature of digital transformation. Bazyliuk et al. (2021) propose a methodical approach to evaluate the efficiency of transforming business processes in engineering enterprises. Their focus on security during transformation processes parallels our study's aim of ensuring safe digital transformation.

Also, Fajsi et al. (2022) link project management maturity with business excellence, suggesting that structured management approaches can significantly impact the successful transformation of businesses, a concept that is relevant to our research on digital transformation. Nam et al. (2019) offer a perspective on business analytics adoption, viewing it through an innovation diffusion lens. This complements our research by providing insights into the adoption process of new technologies and strategies in business, a key component of digital transformation.

Baiyere et al. (2020) explore digital transformation from the perspective of new business process management logics, focusing on the strategic and organizational changes it entails. This work takes a deep dive into how companies can rethink their processes and structures to effectively adapt to digital challenges. In contrast to our study, which focuses on security assessment in the context of digital transformation and intelligentization, Baiyere et al. focus more on change management and process optimization.

Shtangret et al. (2021) discuss the practical aspects of anticipative management in ensuring economic security. Their findings add depth to our understanding of proactive strategies in managing security aspects during business transformations.

Petruk and Shashlo (2022) view digital transformation as a source of both opportunities and threats to business models and enterprise

management systems. Their work includes analyzing the impact of digitalization on organizational structure and strategic planning. While this research highlights the importance of adapting to digital innovation, your work goes further by providing a specific methodology for assessing the security aspects of digital transformation, allowing for a deeper dive into addressing specific security challenges.

In conclusion, these comparative studies collectively underscore the importance of innovative, flexible, and comprehensive approaches to managing security aspects in the rapidly evolving landscape of digital business transformation. They highlight the need for continuous adaptation and reassessment of strategies to effectively navigate the challenges posed by digitalization and intellectualization in various business contexts.

Conclusions

The significant outcome of this study is the identification of key security aspects that influence the digitalization and intellectualization of businesses in the region. More importantly, the research formulated a unique approach for assessing these aspects, contributing to the field's body of knowledge. The innovativeness of the study is highlighted through the proposed model for achieving optimal security in digitalization and intellectualization efforts, specifically within the Ukrainian business context. However, it's important to note the study's limitation in focusing predominantly on the business environment in Ukraine. This specificity may affect the generalizability of the findings to other regions or countries. Looking ahead, the researchers propose expanding the scope of modeling in future studies. While the IDEF0 method was primarily used in this research, exploring the potential of the IDEF3 method could offer more comprehensive insights and applications. In conclusion, this article represents a significant step in understanding and developing strategies for security in the digital transformation of business. It opens avenues for further research, particularly in exploring more diverse modeling methods and extending the study to different geographical contexts.

Bibliographic references

Alazzam, F.A., Aldrou, K.K., & Salih, A.J. (2020). Legal Problems and Challenges Facing Electronic Commerce Contracts and Ways to overcome them in the Jordanian and

Comparative Legislatures. *International Journal of Innovation, Creativity and Change*, 12(9), 323-338. <https://acortar.link/buNHHJ>

- Alazzam, F.A.F., Shakhathreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., & Sylkin, O. (2023). Developing an information model for E-Commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance. *Information Systems Engineering*, 28(4), 969-974. <https://doi.org/10.18280/isi.280417>
- Baiyere, A., Salmela, H., & Tapanainen, T. (2020). Digital Transformation and the New Logics of Business Process Management. *European Journal of Information Systems*, 29(3), 238-259. <https://doi.org/10.1080/0960085X.2020.1718007>
- Bazyliuk, V., Molnar, O., Kyrlyk, N., Vynnychuk, R., & Zavadyak, R. (2021). Methodical approach to evaluation of efficiency of transformation of business processes on engineering enterprises in the context of ensuring security. *International Journal of Safety and Security Engineering*, 11(5), 585-591. <https://doi.org/10.18280/ijss.110510>
- Dubyna, M., Verbivska, L., Kalchenko, O., Dmytrovska, V., Pilevych, D., & Lysohor, I. (2023). The role of digitalization in ensuring the financial and economic security of trading enterprises under the conditions of external shocks. *International Journal of Safety and Security Engineering*, 13(5), 821-833. <https://doi.org/10.18280/ijss.130506>
- Fajsi, A., Morača, S., Milosavljević, M., & Medić, N. (2022). Project management maturity and business excellence in the context of industry 4.0. *Processes*, 10(6), 1155. <https://doi.org/10.3390/pr10061155>
- Ferrari, F. (2022). Are Family businesses a good environment for project management? Non-technological factors affecting project and knowledge management practices within family firms. *Research Anthology on Strategies for Maintaining Successful Family Firms*. IGI global publishing tomorrow research today, 2, 1054-1081. <https://doi.org/10.4018/978-1-5225-9993-7.ch006>
- Fischer, M., Imgrund, F., Janiesch, C., & Winkelmann, A. (2020). Strategy archetypes for digital transformation: Defining metaobjectives using business process management. *Information & Management*, 57(5). <https://doi.org/10.1016/j.im.2019.103262>



- Javaria, K., Masood, O., & Garcia, F. (2020). Strategies to manage the risks faced by consumers in developing e-commerce. *Insights into Regional Development*, 2(4), 774-783.
[https://doi.org/10.9770/IRD.2020.2.4\(4\)](https://doi.org/10.9770/IRD.2020.2.4(4))
- Kim, S., Choi, B., & Lew, Y. (2021). Where Is the Age of Digitalization Heading? The Meaning, Characteristics, and Implications of Contemporary Digital Transformation. *Sustainability*, 13(16), 89-98.
<https://doi.org/10.3390/su13168909>
- Lagodiienko, V., Popelo, O., Zybareva, O., Samiilenko, H., Mykytyuk, Y., & Alsawwafi, F.M.A.S. (2022). Peculiarities of the management of the foreign economic activity of enterprises in current conditions of sustainability. *International Journal of Sustainable Development and Planning*, 17(4), 1215-1223.
<https://doi.org/10.18280/ijstdp.170420>
- Nam, D., Lee, J., & Lee, H. (2019). Business analytics adoption process: An innovation diffusion perspective. *International Journal of Information Management*, 49, 411-423.
<https://doi.org/10.1016/j.ijinfomgt.2019.07.017>
- Petruk, G. V., & Shashlo, N. V. (2022). Digital Transformation: Opportunities And Threats To Business Models And Enterprise Management Systems. In N. G. Bogachenko (Ed.), *AmurCon 2021: International Scientific Conference*, vol 126. *European Proceedings of Social and Behavioural Sciences* (pp. 771-781). European Publisher.
<https://doi.org/10.15405/epsbs.2022.06.85>
- Szwarcz, L. (2023). Rethinking Commercial Law's Uncertain Boundaries. *Duke Law School Public Law & Legal Theory Series*, 2023-12.
<http://dx.doi.org/10.2139/ssrn.4328793>
- Shtangret, A., Korogod, N., Bilous, S., Hoi, N., & Ratushniak, Y. (2021). Management of Economic Security in the High-Tech Sector in the Context of Post-Pandemic Modernization. *Postmodern Openings*, 12(2), 535-552.
<https://doi.org/10.18662/po/12.2/323>
- Shtangret, A., Topalova, E., Polovcev, O., Chornenka, O., & Musiyovskyi, A. (2021). Practical aspects of the use of antisipative management in the process of ensuring the economic security of an enterprise. *Business: Theory and Practice*, 22(1), 202-210.
<https://doi.org/10.3846/btp.2021.13556>
- Sylkin, O., Bosak, I., Homolska, V., Okhrimenko, I., & Andrushkiv, R. (2021). Intensification of Management of Economic Security of the Enterprise in the Post-Pandemic Space. *Postmodern Openings*, 12(1Sup1), 302-312.
<https://acortar.link/HUOih9>
- Sylkin, O., Kryshtanovych, M., Bekh, Y., & Riabeka, O. (2020). Methodology Of Forming Model For Assessing The Level Financial Security. *Management Theory and Studies for Rural Business and Infrastructure Development*, 42(3), 391-398.
<https://doi.org/10.15544/mts.2020.39>
- Sylkin, O., Shtangret, A., Ogirko, O., & Melnikov, A. (2018). Assessing the financial security of the engineering enterprises as preconditions of application of anti-crisis management: Practical aspect. *Business and Economic Horizons*, 14(4), 926-940.
<https://ageconsearch.umn.edu/record/287238/?v=pdf>
- Trokhymets, O. (2020). *Development of national economy in the context of information and digitalization processes*. In book: Challenges and prospects for the development of a new economy at global, national, and regional levels. <https://acortar.link/Cvi0aC>
- Zhou, D., Danshina, S., Kurilova, A., & Lis, M. (2021). The Impact of an Enterprise's Intellectualization on Its Leadership Potential. *Sustainability*, 13(17), 9670.
<https://doi.org/10.3390/su13179670>
- Zybareva, O., Kravchuk, I., Pushak, Y., Verbiivska, L., & Makeieva, O. (2021). Economic and legal aspects of the network readiness of the enterprises in Ukraine in the context of business improving. *Estudios de Economia Aplicada*, 39(5).
<http://ojs.ual.es/ojs/index.php/eea/article/view/4972/4782>
- Zybareva, O., Shylepnytskyi, P., Krylov, D., Arefiev, S., Ozarko, K., & Hryhorkiv, M. (2022). Management of business projects of the enterprise as a factor of increasing international competitiveness in the conditions of global sustainability. *International Journal of Sustainable Development and Planning*, 17(7), 2023-2032.
<https://doi.org/10.18280/ijstdp.170703>