International Journal of Religion
2024
Volume: 5| Number 10 | pp. 856 – 866
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/qdm4yk19

Determination Of Optimal Administrative, Legal and Economic Methods for Managing Artificial Intelligence in The Context of Information Security

Farouq Ahmad Faleh Alazzam[1], Daria Kiblyk[2], Yuriy Kardashevskyy[3], Liudmyla Yaremenko[4] and Svitlana Rodchenko[5]

Abstract

The purpose of the article is to identify the most optimal methods for managing the use of artificial intelligence in educational purposes. For this, the object of research is the information security system of the educational institution. The scientific task involves the formation of a modern method for detecting and organizing the most optimal methods for managing the use of artificial intelligence, which will strengthen the level of information security. As a result of the conducted research, the key methods of managing the use of artificial intelligence in educational purposes were systematized, based on the use of the mechanism of semantic networks and elements of predicate logic, and establishing advantages by means of the methodology of modeling hierarchies and the method of ranking and synthesizing a multi-level model, which allowed forming an information field for the development of measures to ensure information security. The research has limitations in the form of considering only aspects of artificial intelligence and not the entire information system. The prospects for further research are aimed at considering aspects of cybersecurity and cyber threats in education.

Keywords: *Artificial Intelligence, Information Technology, Information Security, Education, Modeling, Main Methods, Economic Security, Risks, Law, Administrative and Legal Aspects*

INTRODUCTION

In the era of globalization and technological progress, digitalization is becoming critical for economic sustainability and business security. Particularly in Eastern European countries, where economic and legal systems are undergoing a period of transformation, it is important to develop adequate mechanisms for managing the risks associated with digital innovation. This study aims to identify and systematize optimal economic and legal techniques that will help improve the level of security in the business environment, taking into account the specifics of the regional context.

In analyzing the business security management system, special attention is paid to studying the integration of modern digital technologies, such as semantic networks and elements of predicate logic. These tools play a key role in identifying, analyzing and organizing data, which in turn allows you to more effectively identify potential threats and develop strategies to neutralize them. This study not only highlights existing methods but also seeks to develop new approaches that meet the unique challenges of the digital era in the Eastern European context.

Digitalization is significantly transforming the economic landscape in Eastern Europe, imposing demands on businesses to adapt to new economic conditions. The introduction of digital technologies requires the optimization of economic and legal management methods in order to ensure business competitiveness and security. One of the key areas where digitalization is making changes is the interaction of businesses with government agencies, in particular in terms of tax administration and regulatory requirements.

[1] Faculty of Law, Jadara University, Irbid, 21110, Jordan; E-mail: alazzamfarouqahmad@gmail.com

[2] Department of Administrative and Legal Disciplines, Donetsk State University of Internal Affairs, Kropyvnytskyi 25000, Ukraine

[3] Odesa State University of Internal Affairs, Odesa, Ukraine

[4] Department of Management and Entrepreneurship, Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, 25006, Ukraine
[5] Department of Finance, Accouting and Business Security, O. M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine

Thanks to digital platforms, companies can more effectively interact with government institutions, simplifying the processes of obtaining the necessary permits, licenses and other regulatory documents. It also paves the way for more transparent and effective compliance monitoring.

In addition, digitalization has an impact on corporate finance management strategies. Automating financial transactions and using analytical tools to process large volumes of data can improve the efficiency of financial decision-making. This allows companies to better manage their assets, optimize costs and improve overall financial stability.

In the digital era, businesses are faced with the need to implement innovative approaches to cybersecurity. The importance of data security is growing as information becomes a key asset for companies. Cybersecurity measures should be an integral part of business strategy, ensuring reliability and trust in electronic control systems.

Digitalization opens up new opportunities for optimizing supply chains. Integrating intelligent systems can lead to more efficient resource management, reduced delivery times and improved overall productivity. Such approaches can significantly improve a business's agility and ability to quickly respond to market changes.

In conclusion, economic and legal optimization in the context of digitalization should be aimed at creating flexible management structures that are adaptive to changes, allowing them to quickly and effectively respond to new challenges and opportunities in the digital economy. This approach will ensure not only survival but also prosperity of business in a dynamic and unpredictable world.

The structure of the article consists of an introduction, a literature review, a description of the methodology, a presentation of the research results, discussion and conclusions. The purpose of the article is to identify optimal economic and legal methods for managing business security in Eastern European countries in the context of digitalisation. For this purpose, the object of study is the business safety management system in Eastern European countries.

LITERATURE REVIEW

In an era of rapid digitalization, economic, business and financial landscapes around the world are undergoing significant transformation. Eastern European countries, with their unique economic and political contexts, face special challenges that require in-depth analysis and innovative approaches. The literature review in this work highlights several studies examining the impact of digital transformation on trade, national security, public administration, business activity and the development of the digital economy. This provides insight into how countries can adapt their strategies to optimize their economic systems, ensure business stability, and protect financial interests in a dynamic, globalized environment.

Thus, Zolkover et al. (2022) will study how digital transformation is impacting the business landscape in Eastern Europe, including the main challenges and opportunities it creates for companies. The authors pay particular attention to the analysis of risks, such as increased cyber threats and data vulnerabilities and also consider benefits, such as improved operational efficiency and expanded market coverage. At the same time, Ghosh et al. (2021) focus on how businesses in the industrial sector can use digital technologies to improve their competitiveness. Using dynamic capabilities theory, the study highlights how firms can adapt to technological change and integrate digital innovation into business models to strengthen financial stability. Krawczak and Szkatuła (2020) analyze the use of intuitive fuzzy sets to model complex information science decisions, which can be useful for businesses trying to optimize their financial and management strategies under conditions of uncertainty. Harahulia et al. (2023) examine enterprise economic security management in the context of digital change. Their research points to the need to develop new management approaches that can help firms manage risk and protect their financial interests in an increasingly digital environment.

Kasianova et al. (2020) focus on the impact of digital transformation on enterprise security, examining how technology is changing traditional approaches to protecting corporate assets. They note the importance of integrating digital tools into corporate security strategies to effectively counter external and internal threats.

Peng (2023) examines the relationship between the digital economy and national security, focusing on cybersecurity and its significance in the context of modern international relations. The study highlights the need to adapt national legal systems to the challenges posed by digital technologies to effectively respond to cybersecurity threats. Irtyshcheva et al. (2022) are engaged in assessing the effectiveness of regional public administration in the context of achieving sustainable development goals. By examining different regions, the study identifies key indicators of governance success that are critical for planning long-term development strategies in the face of climate change and socio-economic transitions.

Megits, Neskorodieva, and Schuster (2020) analyze the impact of the COVID-19 pandemic on trade between Eastern Europe and China. They find that the crisis has brought significant changes to trade flows, requiring countries in the region to rethink their economic strategies and trade relations, especially in the face of increased globalization and an unpredictable international economic environment.

Traucă et al. (2019) discuss the challenges and prospects faced by Central and Eastern European countries due to the digitalization of business activities. The authors examine the processes of adaptation to digital innovation and their impact on the competitiveness of enterprises, which is key to ensuring economic growth in the region.

Banhidi, et al. (2019) conducted a comparative analysis of the development of the digital economy in Russia and the European Union, using the DEA methodology and DESI parameters to assess the effectiveness of digital transformation. They find that significant differences in strategies and levels of adaptation to digital innovation have important implications for shaping economic policies at national and regional levels.

Let see the main gaps in literature today according to the topic of the article (Table 1).

Table 1: The main gaps in literature today according to our topic of the article

№	Gap	Characteristics
1	Lack of integration of interdisciplinary approaches	Many studies focus on specific aspects of digitalization, ignoring the relationships between economic, technological and social factors.
2	Theoretical frameworks	Theoretical frameworks are often used without sufficient empirical support, which can limit the accuracy and objectivity of the conclusions.
3	Insufficient exploration of long-term impacts	Insufficient exploration of long-term impacts: Many studies focus on the short-term effects of digitalization, while the long-term strategic implications of business sustainability and economic development remain under-researched.

Source: own analysis

The scientific task involves the formation of a modern method for identifying and organizing the most optimal methods for managing business security in Eastern European countries in the context of digitalization.

METHODOLOGY

In our study, the use of semantic networks was a key method for analyzing the structure and dynamics of business security management. Semantic networks allow you to visualize the complex relationships between different components of a system, representing them in the form of graphs, where nodes symbolize concepts or entities, and edges display the connections between them. This approach helps identify key areas of risk and interdependencies that may not be apparent in traditional analysis. It also promotes a greater understanding of processes and opportunities to optimize security management strategies.

Additionally, the use of predicate logic in our research makes it possible to formalize information obtained through semantic networks. Predicate logic is used to create logical statements that describe relationships between different aspects of security, allowing you to accurately determine the conditions under which certain events or states are true. This method provides rigour and precision in concluding, allowing for informed risk assessment and the development of effective management strategies.

The hierarchy modelling method is used in our study to prioritize risks and identify key focus areas for management activities. This method allows you to evaluate the importance of various aspects of business

security, ranking them according to their impact on the overall sustainability of the company. This approach facilitates an objective assessment of various threats and the identification of those in need of immediate attention and resources.

The multilevel model ranking and synthesis method is used for detailed analysis and synthesis of data obtained using other methods. This method helps integrate diverse data and findings into a single, multi-layered model that reflects the complexity of a business's security management system. It provides the ability to better understand how different measures and strategies interact with each other and what impact they can have on overall business security.

Together, these methods form a powerful analytical toolkit that allows not only to deeply analyze the existing security situation in a business but also to development effective strategies to improve it. This is especially true in the context of digitalization, where the speed of change and new types of threats require managers to be highly adaptable and responsive.

RESULTS AND DISCUSSION

Managing business security in the context of digitalization in Eastern European countries requires an integrated approach covering economic, financial and business aspects. Here are seven key security management practices we've identified that can be effective in this region:

Digital Infrastructure Development. Improved technology systems, including software and hardware upgrades, are critical to protecting data and systems. Investments in digital infrastructure help reduce technological risks and increase the efficiency of business operations.

Implementation of comprehensive cybersecurity systems. Providing businesses with modern antiviruses, firewalls and other cybersecurity tools is necessary to counter external and internal threats. It is also important to implement incident detection and response (EDR) systems to timely identify and minimize the consequences of cyber attacks.

Big Data Processing and Analysis. Using big data tools allow companies to analyze user behaviour and identify potential threats at an early stage. Data analytics can identify unusual patterns of behavior that may indicate attempts at fraud or tampering.

Regular staff training. Organizing regular trainings and seminars for employees on the principles of cyber hygiene and methods for recognizing phishing attacks and other types of cyber threats provides an important level of internal security.

Strategic risk management. Development of a risk management strategy, including identification, analysis, control and minimization of risks. This helps companies adapt to changes in the external environment and effectively allocate resources to protect the most vulnerable aspects of their operations.

Development of internal policies and procedures. Development and implementation of internal security policies governing access to corporate resources, use of corporate devices and circulation of information within the company. This allows you to create a clear information management structure and reduce the possibility of data leakage.

Developing Partnerships. Collaborate with other organizations and government agencies to share information about threats and best practices. This not only improves overall security, but also allows for the creation of industry standards that improve the effectiveness of cybersecurity measures.

Let's define the set of these methods through the mathematical notation X = {x1, x2, x3, x4, x5, x6, x7}. For describing the semantic network, we will use predicate logic constructs that consist of simple (atomic) predicates and logical connectives: ∧ – logical "and"; ∨ – logical "or"; ← – logical "if"; ∀ – universal quantifier (for all); ∃ – existential quantifier (there exists at least one). Finally, the relationships between management methods in the network will have such a formalized representation: (∀xi) [∃(x1) ← defines (x1, x2) ∧ is assumed (x1, x4) ∧ is conditioned by (x1, x7)]; (∀xi) [∃(x2) ← conditions (x2, x3) ∧ is defined by (x2, x1) ∧ is conditioned by (x2, x4) ∧ is defined by (x2, x5) ∧ is conditioned by (x2, x7)]; (∀xi) [∃(x3) ← conditions (x3, x7) ∧ is conditioned by

(x3, x2) ∧ is conditioned by (x3, x5) ∧ is assumed (x3, x6)]; (∀xi) [∃(x4) ← assumes (x4, x1) ∧ conditions (x4, x2)]; (∀xi) [∃(x5) ← defines (x5, x2) ∧ conditions (x5, x3) ∧ is conditioned by (x5, x6) ∧ receives (x5, x7)]; (∀xi) [∃(x6) ← assumes (x6, x3) ∧ conditions (x6, x5) ∧ conditions (x6, x7)]; (∀xi) [∃(x7) ← conditions (x7, x1) ∧ conditions (x7, x2) ∧ influences (x7, x5) ∧ is conditioned by (x7, x3) ∧ is conditioned by (x7, x6)].

Let's present the scheme of interrelations between the defined management methods for business security management in Eastern European countries in the context of digitalization (Figure 1).

RESULT AND FINDINGS

The model was tested with Partial Least Square-Structural Equation Model (PLS-SEM). A convergent validity assessment was the first step in the process. Hair et al. (2018) suggested using factor loadings, composite reliability, and average variance to verify convergent validity. They also recommend an external load of 0.7. Hair et al. (2019), on the other hand, recommend that social scientists investigate the influence of eliminating markers ranging from 0.40 to 0.70 on average variance extracted (AVE) and composite dependability and keep the reflected indicator if eliminating the external load doesn't improve the measurement above the threshold. There should not be outside load signals lower than 0.40 (Hair et al., 2018). Table I shows that the loading was over 0.7 after removing several items (Hair et al., 2019). Dependability scores ranged from 0.711 to 0.908, well over the minimum of 0.7 needed. For the latent construct indicators, the AVE was 0.567 and 0.632, which is above the needed 0.5 (Hair et al., 2019).

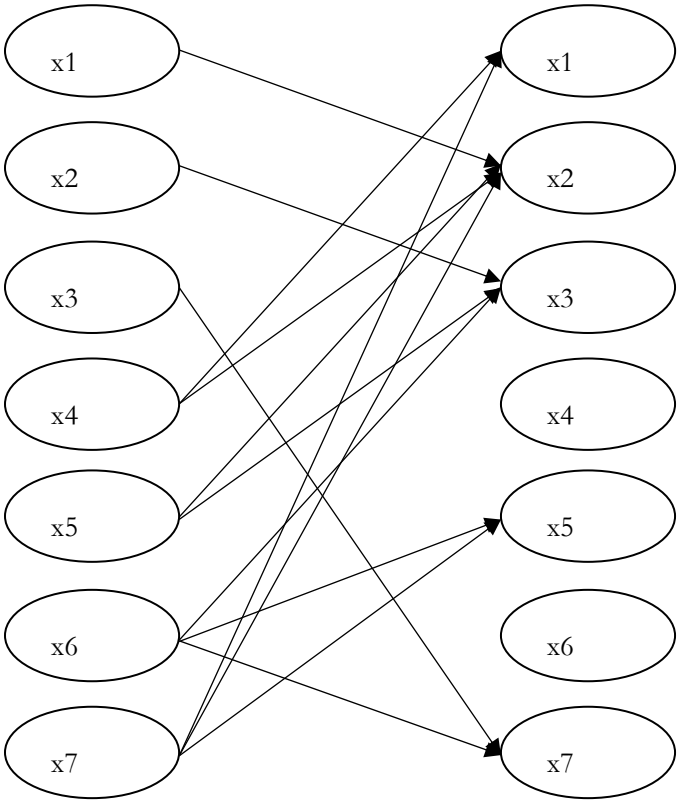

Figure 1: The scheme of interrelations between the defined management methods for business security management in Eastern European countries in the context of digitalization

Source: own analysis

To calculate the total weighted values of direct and indirect influences of various methods and their integral dependency on different educational processes, let's introduce the corresponding notations. Let zij represent

the number of influences or dependencies for the j-th method (j=1,…,n); wi – the weight of the i-th type, where =1,…,7i=1,…,7, since we have 7 management methods for business security management in Eastern European countries in the context of digitalization. Formula (1) provides the calculation of the total numerical priorities of the methods:

$$S_{ij} = \sum z_{ij} w_i, \ (j = 1,7) \quad (1)$$

It is understood that if there are no connections, zij=0. Since, according to the given conditions w3<0 and w4<0, respectively, 0S3j<0 and S4j<0. The final formula for calculating the ultimate numerical priorities of the selected methods would be as follows (2):

$$S_{ij} = \sum z_{ij} w_i + \max S_{3j} + \max S_{4j}, \ (j = 1,7) \quad (2)$$

We will conduct the calculations based on the graph shown in Fig. 1, the analysis of which enables the acquisition of quantitative indicators of connections of various types. As a result, we will obtain data for the preliminary ranking of the defined methods, which determine the transformation of the educational process at the micro-level (Table 2).

Table 2: Preliminary ranking data

j	z_{1j}	z_{2j}	z_{3j}	z_{4j}	S_{1j}	S_{2j}	S_{3j}	S_{4j}	S_{Fj}
1	1	0	2	2	10	0	-20	-10	25
2	1	1	4	2	10	5	-40	-10	10
3	1	3	3	1	10	15	-30	-5	35
4	2	0	0	0	20	0	0	0	65
5	2	1	2	1	20	5	-20	-5	45
6	3	2	0	0	30	10	0	0	85
7	3	1	2	2	30	5	-20	-10	50

Source: own analysis

For the numerical identification of predicates, let's define the coefficients of significance for the predicates, the essence of which will lie in determining the numerical measure of strengthening or weakening the interaction between methods of managing artificial intelligence, depending on the attached linguistic predicates and types of dependencies. Thus, let kip be the coefficients of significance for the predicates that identify the strengthening of influences or dependencies for the p-th predicate of the i-th type of influence. Finally, we will establish the relationship between the coefficients of significance for the predicates as follows: k2pl=(k1pl/2), where l is the predicate number. To take into account the above conditions, we will use the data presented in Table 3, from which we will obtain the linguistic interpretation of predicates of various types of connections between methods and their numerical conditional weights.

To take into account the above conditions, we use the data given in table. 3, from which we obtain a linguistic interpretation of predicates of various types of connections between methods and their numerical weights.

Table 3: Preliminary ranking data

l	Influence predicate	k1,pl	k2,pl	Dependency predicate	k3,pl	k4,pl
1	Defines	4	2	Determined	4	2
2	Forms	4	2	Formed	4	2
3	Causes	3	1.5	to be specified	3	1.5
4	It becomes the basis	4	2	Founded	4	2
5	Presupposes	2.5	1.25	Supposed	2.5	1.25
6	Takes into account	2.5	1.25	Taken into account	2.5	1.25
7	Affects	3	1.5	Receives	3	1.5

Source: own analysis

Finally, to calculate the average values of the action coefficients of an arbitrary factor and given types of connections in the network, it is necessary to determine and present the final expression for calculating the refined weight values of the factors (3):

$$G_{Fj} = INT\left(\sum_{i=1}^{4}\left(k_{ij}S_{ij} + \Delta_j\right)\right), \left(j = \overline{1,7}\right) \tag{3}$$

We summarize the results in the table. 4, in which taking into account the additional impact of predicates provides refined levels of importance for each of the artificial intelligence control methods.

Table 4: Preliminary ranking data

j	k_{1j}	k_{2j}	k_{3j}	k_{4j}	G_{1j}	G_{2j}	G_{3j}	G_{4j}	G_{Fj}
1	4	0	2.7	1.3	40	0	-54	-13	148
2	3	1.5	3.5	3.5	30	7.5	-140	-35	37.5
3	3	0.5	2.8	4.2	30	7.5	-84	-21	107.5
4	2.7	0	0	0	54	0	0	0	229
5	3.5	3.5	3	3	70	17.5	-60	-15	187.5
6	2.8	2.1	0	0	84	21	0	0	364
7	3	4.5	3	1.5	90	22.2	-60	-15	212.2

The result of the ranking is a multi-level model of the priority influence of selected management methods for business security management in Eastern European countries in the context of digitalization at the micro level (Fig. 2).

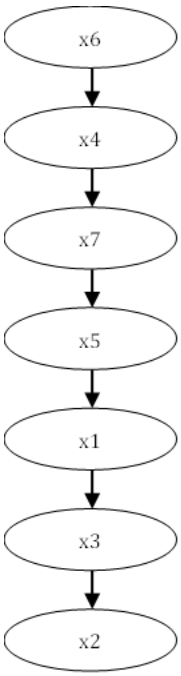

Figure 2: The multi-level model of the priority influence of selected management methods for business security management in Eastern European countries in the context of digitalization

Source: own analysis

The sixth method of business security management, which consists in the development and implementation of internal policies and procedures, turned out to be the most optimal for the realities of Eastern European countries after applying our methodology. The use of this method made it possible to effectively structure access to information, control internal communications and ensure strict compliance with security standards. Clearly defined procedures for the use of corporate resources and information circulation minimize the risks

of unauthorized access and data leakage. Thanks to our methodology, organizations were able to implement effective policies that are adapted to the specific conditions and challenges of the digital environment in the region, which significantly increased their ability to protect critical information and maintain stable operations in the face of constantly changing threats.

DISCUSSION

Comparing the results of our study with existing work is critical to better understand and evaluate the effectiveness of business security management practices in the context of digitalization. This comparison not only allows us to determine the novelty and contribution of our work to scientific discourse, but also helps to identify possible gaps in research that could be revised or improved. Such analysis also helps establish how our research findings correlate with global trends and practices, providing important context for developing recommendations useful to businesses in Eastern Europe and other regions. Paying attention to these aspects not only increases the scientific value of our work, but also contributes to the formation of practical approaches to risk management in a highly dynamic digital environment.

Thus, in our research we focus on optimizing business security management practices in Eastern European countries in the context of digitalization. Our approach includes the use of semantic networks and predicate logic, which allows us to deeply analyze and systematize key risks.

While Caputo et al. (2019) explore boundary management in business processes. They focus on management flexibility and adaptation to change, which is important for business sustainability. Our research is distinguished by its depth of focus on security and the use of specific analytical tools, allowing for more targeted identification and management of risks in the digital context.

Fonseca (2018) examines the broader concepts of Industry 4.0 and the digital society, emphasizing the possible benefits of digitalization of business and society. Our research, in turn, focuses on a specific aspect of digitalization of business security, which allows us to develop tailored solutions for this problem in detail.

An interesting study by Menchini et al. (2022), analyzing strategic opportunities for digitalization of business models. While their focus is on strategic changes in the management of companies, our research more specifically addresses security issues in the context of digital transformation, which is critical in today's digital environment.

Bocean and Vărzaru (2023) examine the impact of digital transformation on economic efficiency and sustainability in EU countries. While their analysis includes a wide range of economic indicators, our research contributes to the understanding of how digitalization specifically impacts business security by providing strategies for minimizing risks.

Hess et al. (2015) and Luo (2022) explore digital transformation strategies and digitalization risks in international business. While these studies examine general strategies and risks, our study makes a unique contribution by focusing on risk management practices specialized to the Eastern European context in the context of digitalization, allowing us to more effectively address the specific challenges of this region.

Saed et al. (2023) in their study examine the cybersecurity challenges that businesses face during digital transformation, emphasizing the need to improve organizational resilience. They are developing a series of recommendations that can help businesses adapt to growing cyber threats. This study has similarities to ours in that we also focus on risk management in the digital environment. The difference lies in the specific focus on business security systems in Eastern Europe, where we additionally take into account regional characteristics and needs.

Hai et al. (2021) discuss the opportunities and challenges facing leaders in developing countries in responding to the COVID-19 pandemic through digital transformation. Their findings point to the potential benefits of digitalization to support operational flexibility and recovery. Our research examines similar topics, but with a security focus, identifying strategies that help minimize risks from digital threats.

Simon and Omar (2020) analyze cybersecurity investments in a supply chain context, examining interactions between different parties and strategic attackers. They point out the importance of coordination between all participants in the chain to ensure everyone's safety. Our research extends this perspective by integrating these approaches into the broader context of digital business transformation in Eastern Europe, highlighting specific methods and technologies that can be used to achieve end-to-end security. Goerzig and Bauernhansl (2018) explore enterprise architecture to support digital transformation in SMEs. They emphasize the importance of adapting technological infrastructures to improve competitiveness. Our research is more focused on security, but we use similar approaches to analyze technology solutions that can effectively manage risk in digital transformation, emphasizing the importance of a strategic approach to digital security.

Lets mark our main innovation in our article compare to others (Table 5).

Table 5: The main innovation in our article compare to others

The main results	Characteristics
Regional Focus	Our research focuses on Eastern European countries, a region that is often under-focused in global research. This provides an important contribution to the literature as we analyze how digitalization impacts business security in contexts that have unique cultural, economic, and political characteristics.
Innovative Analytical Approach	Using semantic networks and predicate logic to analyze business security is a relatively new approach in the field. These techniques provide a deeper understanding of the complex interactions and risks that exist in today's business environment and offer a more systematic and accurate solution to security management problems.
Practical Security Implications	Our research results not only enrich the theoretical framework on cybersecurity and risk management, but also have significant practical implications. They help enterprises and government organizations develop more effective security strategies based on detailed and comprehensive analysis of potential threats and vulnerabilities.

Source: own analysis

Comparison of the results of our study with existing works confirms the relevance and contribution to scientific novelty in the field of business security management in the context of digitalization. Our approach, integrating the use of semantic networks and predicate logic for risk analysis, has proven effective in identifying and systematizing threats that pose a particular threat in the digital era. This highlights the importance of our work in developing sound security management strategies that take into account the specifics of the regional business environment in Eastern Europe. This regional focus helps provide more precise and effective solutions to cybersecurity and risk management challenges, demonstrating significant potential for translating our findings into practice.

CONCLUSION AND RECOMMENDATION

The digitalization of the economy poses significant challenges to business security in Eastern European countries, where technological progress and legal regulation are often out of step. The main problems in this area are the insufficient level of cybersecurity, high dependence on outdated technologies and shortcomings in the legal regulation of digital transactions. These challenges are exacerbated by volatile economic conditions and political uncertainty, forcing businesses to seek ways to adapt to rapidly changing market conditions.

Additionally, the financial vulnerability of companies in these regions is exacerbated by currency fluctuations and international economic sanctions. Such factors complicate the management of capital investments and credit risks, requiring new approaches to financial planning and risk analysis. The scientific research, the results of which are discussed in this article, focused on identifying and systematizing optimal economic and legal methods for managing business security in the context of digitalization. Based on an analysis of the existing conditions and business needs in Eastern European countries, a number of methods have been identified that can help improve the level of security in these conditions.

An important part of the study was the use of advanced technological solutions for data analysis, which made it possible to identify key risk areas and opportunities for minimizing them. Our approach allowed us not only to identify weaknesses in business security systems, but also to develop recommendations for eliminating them, adapted to the specifics of the regional market.

Thanks to the research, it was also possible to develop strategic directions for further improving the security policy, including strengthening the legal framework and introducing modern IT solutions. These steps involve attracting appropriate resources and investments that will help create a more secure and resilient business environment.

The conclusion of our study highlights the importance of an integrated approach to business security management that considers both technological and economic aspects. This approach is key to adapting to the changing conditions of the global digital economy and ensuring business sustainability in the challenges of the 21st century.

One of the main obstacles of the study is the limited application of the findings outside the context of Eastern European countries. Although the methodologies studied make significant contributions to the understanding of business security management processes in this region, they may not take into account the unique economic, cultural, and technological characteristics of other geographic areas. Such geographic limitations may impact the generalizability and application of findings to a broader international level, limiting the ability to scale up and implement recommended practices globally.

Additionally, the specificity of the analytical tools used, such as semantic networks and elements of predicate logic, requires researchers to have a high level of specialization and deep knowledge in these areas, which can become a barrier for other researchers wishing to use or expand the research. This technical limitation may make it difficult to widely disseminate and implement the developed techniques into practice, since specialized training and resources are required to effectively implement the proposed solutions.

Future research in this area could focus on several key aspects to improve and extend current findings. First of all, it is recommended to conduct a comparative analysis with other regions of the world, which will allow us to evaluate the universality and adaptability of the proposed methods. This approach will not only improve understanding of global business security challenges, but will open up new opportunities for international cooperation and integration of best practices.

The issue of expanding the theoretical base for integrating economic and legal frameworks into digital governance mechanisms also remains relevant. Studying and adapting international experience in these areas can bring new ideas and solutions useful for strengthening the legislative and institutional framework for business security management.

Ultimately, it is important to continue to develop methods for assessing the impact of technological innovation on economic security, including the potential risks and challenges facing companies in the digital age. These research perspectives will not only enrich the academic literature, but will also help shape practical recommendations for business and policymakers, tailored to the rapidly changing conditions of a globalized world.

REFERENCES

Akimova, L., Akimov, O., Maksymenko, T., Hbur, Z., Orlova, V. (2020). Adaptive management of entrepreneurship model as a component of enterprise resource planning. Academy of Entrepreneurship Journal, 26(3): 1-8.

Banhidi, Z., Dobos, I., Nemeslaki, A. (2019) Comparative Analysis of the Development of the Digital Economy in EU Measured with DEA and Using Dimensions of DESI. University Journal of Economic Studies 35(4), 588-605, http://dx.doi.org/10.21638/spbu05.2019.405

Bocean, C.G., Vărzaru, A.A. (2023) EU countries' digital transformation, economic performance, and sustainability analysis. Humanit Soc Sci Commun 10, 875. https://doi.org/10.1057/s41599-023-02415-1

Caputo, A., Fiorentino, R., and Garzella, S. (2019) From the boundaries of management to the management of boundaries. Business Process Management Journal 25(3), 391-413, http://dx.doi.org/10.1108/BPMJ-11-2017-0334

Fonseca, L.M.(2018) Industry 4.0 and the digital society: concepts, dimensions and envisioned benefits. Sciendo 12(1), 386-397, http://dx.doi.org/10.2478/picbe-2018-0034

Ghosh, S., Hughes, M., Hodgkinson, I., & Hughes, P. (2021). Digital transformation of industrial businesses: A dynamic capability approach. Technovation, 102414. https://doi.org/10.1016/j.technovation.2021.102414

Goerzig, D., Bauernhansl, T. (2018). Enterprise architectures for the digital transformation in small and medium-sized enterprises. Procedia CIRP, 67, 540–545. https://doi.org/10.1016/j. procir.2017.12.257

Hai T.N., Van Q.N., Thi Tuyet M.N. (2021) Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. Emerg. Sci. J. 5,21–36. https://doi.org/10.28991/esj-2021-SPER-03.

Harahulia, A., Suslov, V., & Horovoy, O. (2023). Management of economic security of enterprises in the context of digital transformation. Baltic Journal of Economic Studies, 9(5), 87-93. https://doi.org/10.30525/2256-0742/2023-9-5-87-93

Hye, Q. M. A. (2012). Long term effect of trade openness on economic growth in case of Pakistan. Quality & Quantity, 46(4), 1137-1149.

Hye, Q. M. A., & Wizarat, S. (2013). Impact of financial liberalization on economic growth: a case study of Pakistan. Asian Economic and Financial Review, 3(2), 270.

Islam, F., Hye, Q. M.A., & Shahbaz, M. (2012). Import-economic growth nexus: ARDL approach to cointegration. Journal of Chinese Economic and Foreign Trade Studies, 5(3), 194-214.

Hye, Q. M.A., & Boubaker, H. B. H. (2011). Exports, Imports and Economic Growth: An Empirical Analysis of Tunisia. IUP Journal of Monetary Economics, 9(1).

Hess, T., Matt, C., Benlian, A. (2015). Digital Transformation Strategies. Business & Information Systems Engineering, 57(5), 339–343.https://doi.org/10.1007/s12599-015-0401-5

Irtyshcheva, I., Pavlenko O., Boiko Y., Stehnei M., Kramarenko, I., Hryshyna, N., & Ishchenko, O. (2022). Evaluation of efficiency of regional public governance in the context of achieving goals of sustainable development. Management Theory and Studies for Rural Business and Infrastructure Development. 44(4), 497–505. https://doi.org/10.15544/mts.2022.49

Kasianova, N. V., Kravchuk, N. M., & Koval, Y. L. (2020). Enterprise security under digital transformation of economics. Modern Economics, no. 20(2020), 124–129. DOI: https://doi.org/10.31521/modecon.V20(2020)-20

Krawczak, M., & Szkatuła, G. (2020). On matching of intuitionistic fuzzy sets. Information Sciences, 517, 254-274. https://doi.org/10.1016/j.ins.2019.11.050

Luo, Y. (2022) A general framework of digitization risks in international business. J Int Bus Stud 53, 344–361. https://doi.org/10.1057/s41267-021-00448-9

Megits, N., Neskorodieva, I., & Schuster, J. (2020). Impact assessment of the COVID-19 on trade between Eastern Europe and China. Journal of Eastern European and Central Asian Research, 7(3), 385-399. https://doi.org/10.15549/jeecar.v7i3.579

Menchini, F.; Russo, P.T.; Slavov, T.N.B. and Souza, R.P.(2022) Strategic capabilities for business model digitalization. Rege-Revista De Gestao 29(1), 2-16, http://dx.doi.org/10.1108/REGE-10-2020-0086

Peng, S. (2023). Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions. AJIL Unbound, 117, 122–127. https://doi.org/10.1017/aju.2023.18

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors (Basel, Switzerland), 23(15), 6666. https://doi.org/10.3390/s23156666

Datsii, O., Levchenko, N., Shyshkanova, G., Dmytrenko, R., Abuselidze, G. State decoupling audit of low-carbon agricultural production / Rural Sustainability Research, 2021, 45(340), стр. 94–112

https://doi.org/10.2478/plua-2021-0011

Simon J., Omar A. (2020) Cybersecurity investments in the supply chain: Coordination and a strategic attacker. Eur. J. Oper. Res.282, 161–171. https://doi.org/10.1016/j.ejor.2019.09.017

Traşcă DL, Ştefan GM, Sahlian DN, Hoinaru R, Şerban-Oprescu G-L. (2019) Digitalization and Business Activity. The Struggle to Catch Up in CEE Countries. Sustainability. 11(8), 2204. https://doi.org/10.3390/su11082204

Kostiukevych, R., Mishchuk, H., Zhidebekkyzy, A., Nakonieczny, J., & Akimov, O. (2020). The impact of european integration processes on the investment potential and institutional maturity of rural communities. Economics and Sociology, 13(3), 46-63. https://doi.org/10.14254/2071-789X.2020/13-3/3

Zolkover, A., Petrunenko, I. ., Iastremska, O. ., Stashkevych, O. ., & Mehdizade, M. M. (2022). Benefits and Risks of Digital Business Transformation: The Example of Eastern Europe Countries. Journal of Eastern European and Central Asian Research (JEECAR), 9(2), 344–356. https://doi.org/10.15549/jeecar.v9i2.910