Stability of Financial Institutions Under the Influence of Cyber Threats

Volodymyr Polishchuk [1*], Nataliia Fedirko [2], Dymytrii Grytsyshen [3], Kyrylo Ohdanskyi [4], Volodymyr Kotkovskyy [5]

[1] Interregional Academy of Personnel Management, Kyiv, Ukraine.
[2] Department of National Economy and Public Administration, Faculty of Economics and Management, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine.
[3] Department of National Security, Public Management and Administration, Faculty of National Security, Law and International Relations, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine.
[4] Department of Economics and Economical Security, University of Customs and Finance, Dnipro, Ukraine.
[5] Department of Socio-Political and Economic Disciplines, Kryvyi Rih Faculty of the National University "Odesa Law Academy", Kryvyi Rih, Ukraine.
[1] **Corresponding author:** Polishchuk.Volodymyr.20@proton.me

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: The issue of the impact of cybersecurity is a top priority for the functioning of a financial institution. Therefore, its provision becomes a priority in organizing the further activities of the institution itself. The article aims to analyze the current trends in ensuring the cybersecurity of financial institutions and its role in their functioning. The paper describes the theoretical foundations of the cyber protection concept. The authors also outline the specifics of cybersecurity and the leading technological solutions for achieving these goals. Special attention is paid to modern, innovative solutions to maintain the stability of financial institutions and the possibility of further development. An important area of research is the disclosure of the practical experience of information corporations in providing technical solutions to ensure the security of financial transactions and support the global financial system. The study presents the experience of Ukrainian financial institutions that use variable digital defense strategies and maintain their functionality based on an effective cybersecurity system in the context of a global military conflict. The results of the study include a detailed profile of effective practical solutions to ensure the stability of financial institutions based on the implementation of blockchain technologies. The authors pay attention to the issue of modern software, hardware, and management solutions to improve the quality of cybersecurity in the context of growing cyberattacks and digital threats to the stability of financial institutions. The research findings may be helpful for further analytical studies on the effectiveness of cybersecurity and the stability of financial institutions.

Keywords: cybersecurity, cryptography, data encryption, banking institutions, financial sector, data centers, digital protection.

Introduction

The modern development of digital technologies, e-commerce, and the automation of financial institutions' activities offers several advantages for efficient management and user convenience in financial services. However, ensuring cybersecurity remains a pressing issue, as the digital environment remains vulnerable in today's technological world.

Over the past decade, there has been an increase in malicious attacks on financial institutions, cryptocurrency exchanges, and various financial service providers [1]. Therefore, the challenge of finding effective technological solutions and improving the functioning of financial institutions is crucial for their continued development.

The most popular technological solutions include:

- variable digital storage systems, similar to cloud systems;
- the use of big data analytics;
- the implementation of data backup systems;

– data encryption through cryptographic methods.

However, regardless of the extensive measures aimed at safeguarding the integrity of financial processes and data security, a key factor is the combination of all security aspects. It includes risk mitigation and reduction, minimizing human error risks, leveraging legal frameworks for cybersecurity, connecting to global financial networks, and internal server system decentralization.

The implementation of low-level architectural software security is the most effective means to ensure the stability of financial institutions' operations [2]. It involves creating technological solutions for digital protection at the hardware level. The conflict in Ukraine has sparked global competition among various world powers. It has led to the need for enhanced cybersecurity and the development of effective management methods and models for financial institutions.

The article focuses on the impact of cybersecurity on the functioning of financial institutions and practical solutions to ensure a country's macroeconomic stability. They are illustrated through real examples from financial institutions.

Literature review

The specifics of cybersecurity's impact on the stability of financial institutions is an essential debatable issue. It involves using and implementing various digital technologies, including hardware and software. In particular, Abdel Hakeem et al. [3] notes that the current cybersecurity policy is a top priority worldwide. This is due to the rapid restructuring of the traditional economy into a digital one. It leads to an inadequate state of security of data storage, documentation, and the life support of the financial institution system [4]. According to Hodula [5], cybersecurity is a global challenge for the entire world. It should use decentralized data storage systems and implement a range of cryptographic methods in its business activities to ensure the stability of further operations. According to Levytska et al. [6], the key factor in cybersecurity is to counteract cyberattacks on web resources, mobile applications, and clients of a financial institution. This involves customizing software and technologies for websites. In addition, according to Anand et al. [7], the implementation of effective server and data center security cannot guarantee complete security.

For this reason, the researcher suggests using cloud storage for a more reliable system of managing personal data and financial transactions. Most of the information giants of the modern world, as noted by Buchak et al. [8], use their own digital infrastructure to provide services to improve the quality of security of financial institutions. However, in the context of the emergence of innovative technologies and the rapid development of technical means, ensuring the complete protection of personal data is a difficult task [3].

According to Nikonenko et al. [9], the most popular means of ensuring personal data protection is the use of encryption systems and a single blockchain system. Melnyk et al. [10] agrees with this argument and believes that establishing a blockchain for the global financial network and using it to eliminate the possibility of stealing or falsifying financial institution data is an innovative solution to ensure financial institutions' stability. According to Kotidis and Schreft [11], the practice of blockchain development and integration is becoming increasingly popular and can be applied to public administration, key government agencies, and the financial sector, which will be reliably protected from external influence. Cerasi et al. [12] believes that the practice of implementation will constantly evolve and cover new sectors of the financial environment. Sumets et al. [13] argues that an essential factor in financial institutions' cybersecurity is to conduct specialized training for the staff on digital literacy and work with information technology. Although automation is popularized, most cyberattacks are successful due to the human factor. Novak et al. [14] studied this issue and stated that the creation of guidelines for working in a financial institution and conducting training activities is equally important as the use of modern digital security technologies.

Consequently, among scientists, the issue of the impact of cybersecurity on the stability of financial institutions is seen as essential and relevant, and it requires further investigation [15].

The study aims to analyze current trends in cybersecurity and its impact on the stability of financial institutions. The article also seeks to explore the support of their vital functions in the context of increasing digital threats. The main research goal is to analyze the practical experience of large financial institutions in formulating their own cybersecurity strategy and to determine the features of technical solutions to support these tools. An important area of analysis is to define the current trends in digital technological solutions among financial institutions aimed at ensuring their own security in the digital space and its further support through the implementation of effective digital and innovative solutions. The article analyzed theoretical, methodological, and practical approaches to cyber protection and digital tools that help maintain the stability of financial institutions.

Materials and methods

In writing this article, the authors analyzed the theoretical features of the operation of financial institutions and determined the impact of cybersecurity on the stability of their activities. For theoretical analysis, the authors used materials from periodicals on the review and peculiarities of the functioning of technological solutions in cybersecurity. In addition, they generalized the most popular practices and solutions to ensure the stability of financial institutions. Based on the use of analytical reports of such global organizations as ICAAN (International Corporation for Assurance of Cyber Security), FIRST (Computer Incident Response and Coordination Team), and ENISA (European Cyber Security Agency), they have made comprehensive assessments of the peculiarities of cybersecurity impact on the functioning of modern financial institutions.

The research methodology involves the analysis of technical reports, popular statements from organizations, and the systematization of the use of relevant technologies for digital protection. In the context of escalating geopolitical conflicts, as exemplified by the war in Ukraine, the authors analyzed open data from official resources of financial institutions to implement methods for strengthening cybersecurity and stability of bank operations. By using this information, the article builds a strategy for Ukrainian financial institutions (banks). This strategy is designed to ensure digital protection and stability of the financial structure under constant cyberattacks. Also, the authors present specific technical solutions adopted by these institutions to improve the quality of digital security.

Applying such an analytical method in the article provides an opportunity to assess the most optimal means of ensuring the financial sector's stability among the largest institutions (banking institutions). In practice, they make some radical decisions to ensure their own digital security and counteract cyber threats. The proposed research methodology allowed us to obtain results on the stability of financial institutions and the role of cybersecurity in their activities.

Results

The concept of cybersecurity, as proposed by Atstaja et al. [16], is an effective means for minimizing risks in the digital environment. It encompasses a set of actions and technological tools to ensure the efficiency of a web resource with access to the internet. The modern development of digital technologies encourages the search for effective and efficient solutions to enhance the confidentiality of personal data and protect the organizational and commercial business processes of an institution, organization, or any structure from external interference [17]. The data transmission using OSI network protocols is the fundamental factor in establishing cybersecurity. It has seven layers responsible for connections between various digital carriers. Additionally, financial institutions or other organizations can operate on their local networks, which do not require additional internet network connections. However, in such conditions, cybersecurity is related to the reliability of configuring hardware and software for data flow and structuring the information environment.

The contemporary technological development in the financial market has led to the growing significance of e-commerce, improving the quality of service for people and legal entities through electronic transactions. Nevertheless, ensuring the efficiency of data management, verification of the legitimacy of data transactions, and protection against external interference are top priorities for financial institutions, as well as for the state. The latter contains a set of electronic registers that can be used as tools for managing digital security.

The concept of the impact of cybersecurity on the stability of financial institutions is of paramount importance, as it determines the rules of their overall operation. According to Ceylan [18], the operation of a financial institution is only possible with prior planning for the legal nature of its activities and the protection of personal data in compliance with the requirements of regulatory and supervisory authorities. For instance, when planning a financial institution as a commercial organization, a series of digital solutions is determined to conduct its activities in the financial environment further. Firstly, plans are made for automated systems for accounting, verification, and the functionality of financial transactions involving currency, precious metals, and other financial assets. Secondly, such organizations need to create an existing digital infrastructure that can utilize cloud technologies such as Oracle, Dropbox, and various other alternative technological solutions. An essential factor in ensuring the planning of a financial institution's activities is the minimization and prevention of risks, creating a relevant structural department responsible for addressing these issues [19, 20]. According to this approach, the impact of cybersecurity on a financial institution is crucial and requires high-quality technological solutions. Table 1 provides more detailed information regarding this issue.

Table 1. The impact of cybersecurity on the stability of financial institutions, analysis, and measures to prevent risks

Parameter	Impact on financial institutions' stability	Measures to improve cybersecurity
Cyber attacks	Increased risk of financial losses, loss of reputation, and possibility of financial failure	Regular security audits, staff training, recovery plan development
Legislation and regulations	Regulation of cybersecurity as a requirement for financial institutions, an impact on operations	Complying with requirements and creating security policies
Internal Security	Strengthening security and control measures to prevent cyber attacks	Monitoring and improving security systems
Technological risks	The impact of innovative technologies on the increase/decrease of risk	Risk assessment, improvement of procedures, and application of advanced technologies
Interconnection of institutions	Cooperation and information exchange between financial institutions for collective protection	Developing standards and collaboration for cybersecurity
Monitoring and recovery	Monitoring systems and backup recovery to detect and eliminate cyber threats	Constant monitoring and recovery plans after an attack

Source: compiled by the authors

The measures listed in Table 1 are widely used by global payment systems and various financial institutions that provide financial services and settlement functions. However, depending on their location and operational regions, they are subject to norms governing the digital security of their own infrastructure and financial operations. In particular, the International Organization for Standardization (ISO) has a set of requirements for the quality of cybersecurity standards and key solutions. They include data encryption, quarterly updates, and service maintenance, monitoring of their data centers, and the use of various antivirus programs to ensure uninterrupted operation of financial institutions, and more. A Federal Office for Cybersecurity and Infrastructure (CISA) was established to investigate the most significant cyberattacks in today's digital world. CISA aims to improve the overall digital environment by developing software and strengthening the protection of financial institutions.

The impact of cybersecurity on the stability of financial institutions is difficult to overstate, as it determines the continued operation of the entire structure. It must comply with standards both on a domestic level – the country's legal environment, and a global level – international organizations that create relevant regulations. Blockchain technology has become an innovative means of ensuring the stability of financial institutions and has been widely integrated into all levels of government. The use of such a system in financial institutions significantly reduces the risk of external influence and malicious digital actions. In China, the United States, and Switzerland, blockchain systems are commonly applied to the majority of corporate organizations and financial institutions to ensure their stability [21].

The conflict in Ukraine has posed a series of global challenges for digital security. Ukrainian banks, as some of the largest financial institutions in the country, are responsible for safeguarding customers' personal data and ensuring the stability of their service offerings. However, they also serve as a means of national strategic security in a financial context. Therefore, the timely adoption of operational and technical solutions, as well as security planning, has enabled the stability of Ukraine's financial system during global economic and political crises.

Management decisions aimed at diversifying risks and avoiding them, using cloud services and authentication technologies, as well as strengthening financial monitoring were key factors in the cybersecurity impact. Furthermore, every major Ukrainian bank conducted a series of trainings on digital literacy and digital security skills during the war. The key measures taken by the largest banking institutions during the war in Ukraine in 2022–2023 are shown in Table 2.

Table 2. Measures and technical solutions taken by Ukrainian banks to strengthen their cybersecurity during the war

Name of the Bank	Measures for Ensuring Cybersecurity	Technical solutions
Privatbank	Establishing a cryptographic connection for a secure data exchange between branches and the bank's central server.	The location of its own data centers in Europe provides storage facilities with reliable data encryption.
Monobank	Implementation of network firewalls and intrusion interception systems to detect and block unauthorized access to the bank's systems.	Application of multi-level user identification and creation of decentralized database systems operating in cloud storage.
Universal Bank	Enhancing network security by regularly monitoring the network and detecting unusual activity.	The use of a data backup system and automated recovery in case of a cyberattack.
Oschadbank	Improving personnel authentication and authorization procedures.	Ensuring the physical security of server rooms and conducting awareness campaigns among users to protect their data and improve the quality of its use.
UkrGasBank	Data encryption during transactions and its storage on servers with restricted access.	Relocation of data centers to countries with stricter cybersecurity standards as another level of protection.

Source: compiled by the author

The measures employed by Ukrainian banks during the war in Ukraine have become a decisive factor in ensuring the financial stability and functioning of institutions. The experience of PrivatBank is particularly significant. From 2019 to 2020, the bank implemented a series of digital solutions, including changes in the location of data centers and the integration of various cloud technologies to ensure the continuity of its operations. In 2022, the bank was able to provide data backup and encryption using cryptography. It utilized multiple low-level data transmission protocols and encrypted confidential information. The experience of Ukraine's largest state-owned bank can serve as a real-life example of a financial institution's functioning in the most crisis-ridden situations.

Crisis management aimed at ensuring digital protection is a vital managerial factor for the stability of a financial institution's operations. In today's world, automation has fewer shortcomings, but the effectiveness of organizational and administrative environments remains a significant issue. This involves enhancing the competency of employees through training and instructions in various crises.

Comprehensive management in cybersecurity, both on a technological and managerial level in modern financial institutions, plays a pivotal role from the perspective of national security, customer, and corporate aspects. For this reason, it is particularly crucial in the context of the accelerated development of data encryption technologies, such as TDEA. Such data encryption technologies involve symmetric encryption. This method focuses on concealing the key used for both encryption and decryption. However, in 2023, with the development of artificial intelligence, this method was enhanced by implementing additional technical means. The latter includes AES encryption, an innovative safeguard for internal file access. This method is utilized by the U.S. government and several financial institutions to enhance the digital protection of critical information.

Therefore, the contemporary impact of cybersecurity on the stability of financial institutions plays a pivotal role as it determines their planned and operational activities. Data encryption methods and complex algorithms that can be built on blockchain systems are contributing to the improvement of modern digital protection. Ukrainian financial institutions have demonstrated effective management of technological solutions to minimize risks from existing cyberattacks. However, despite the effectiveness of current cybersecurity measures in financial institutions, this field requires continuous updating due to the rapid development of digital technologies, artificial intelligence, and Big Data technologies [22].

Discussion

Based on the conducted research, it can be stated that the practice of using technical cybersecurity tools is a key means of ensuring the stability of financial institutions. These tools include cryptography, encryption, efficient server configuration, data center relocation, improving authentication quality, and other methods. In the context of modern technological development, the issue of the effective use of digital tools and data integrity preservation is a top priority for any country, as it is a matter of national and strategic security. According to Hooks et al. [23], the future prospects of data protection will increasingly shift towards blockchain systems. The latter can effectively store information about both financial institution clients and a range of internal organizational documents. According to him, the practice of enhancing the cybersecurity of financial institutions should be integrated into the global financial network. The blockchain will be the foundation of this network.

Furthermore, with the advancement of Big Data analysis technologies, implementing data protection becomes a more straightforward task for the modern world, necessitating further analytical and technical research. The experience of developed countries indicates that implementing blockchain systems in both financial institutions and government organization management is an effective method for avoiding corruption and cyberattacks. They are serving as the best way to ensure digital data security.

The critical aspects of the impact of cybersecurity on the stability of financial institutions include:

- the management of encrypted protocols;
- the use of a range of SSL certificates;
- the ability to form data transmission at all levels of the OSI model with appropriate encryption.

Hu et al. [22] mentions that to transmit data effectively, it is necessary to use private servers and have access to data centers with additional protection in the form of cloud storage. Prospective research may include the following measures:

- the examination of cloud storage systems integrated directly into the activities of financial institutions;
- an analysis of hardware characteristics;
- a comparative evaluation of leading products in the information industry, such as Oracle, Dropbox, or any others available in financial institutions.

The conflict in Ukraine has exacerbated the geopolitical struggles in the world, where cyberspace has become a separate battlefield. The analysis conducted in this article regarding the practical and technical solutions of Ukrainian financial institutions (banks) for ensuring the efficiency of cybersecurity may serve as a model for improving the policies of financial institutions worldwide.

According to Borodina et al. [24], modern financial institutions should strengthen their digital infrastructure. They should have several levels of protection for both client personal data and their own systems. The experience of European Union countries may be intriguing for studying the presence of a local European-style financial network with reserve data centers, servers, and a range of digital solutions for effective operation. Therefore, an analysis of the capabilities of backup systems, additional power supplies, and the definition of basic characteristics for this infrastructure at the hardware level may be of technical importance for financial institutions globally.

Conclusion

Thus, it can be concluded that the concept of cybersecurity involves maintaining the confidentiality of information and countering digital attacks, as well as any external influence aimed at their theft or falsification. Typically, cybersecurity can be achieved through the following means:

- a software;
- a range of technical hardware solutions related to digital infrastructure, server support, and data centers;
- the implementation of regulatory frameworks for the handling of personal customer data in financial institutions and policies regarding their usage.

With the rapid digital development, modern data encryption and cryptographic methods have become the most common among financial institutions. They aim to provide quality services and create a secure environment for

storing and working with data. Cryptography has become the most popular means of safeguarding data that requires effective encryption. Besides, the adoption of cloud technologies serves as a means of protecting data from physical carriers. Such a decentralized system is most popular in the United States, China, Germany, Switzerland, and many other countries considered to be global financial centers.

The article addresses the issues of avoiding cyberattacks and strengthening their means to ensure the most effective security for client communication channels, such as websites, mobile applications, online platforms, and terminals [25, 26]. The implementation of digital facial recognition systems, transaction tracking, and verification of their legality is an effective method to prevent the negative consequences of digital threats. The war in Ukraine has resulted in a powerful attack on many Ukrainian banks and other financial institutions operating in Ukraine. However, despite the aggressor country, financial institutions are implementing various effective strategies, including:

- geographic diversification of data center locations;
- the use of backup systems;
- efficient proprietary software;
- cloud system integration.

These methods can help to ensure the cybersecurity of financial institutions in the context of digital warfare, which can be helpful for the entire world.

References

[1] Karim, S., Naeem, M. A., Mirza, N., & Paule-Vianez, J. (2022). Quantifying the hedge and safe-haven properties of bond markets for cryptocurrency indices. *The Journal of Risk Finance, 23*(2), 191–205. https://doi.org/10.1108/JRF-09-2021-0158

[2] Karlzén, H., Granlund, H., & Wedlin, M. (2018). Operations in the cyber domain – an inventory of Swedish research. FOI-R-4594. *Swedish Defence Research Agency*.

[3] Abdel Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security requirements and challenges of 6G technologies and applications. *Sensors, 22*(5), art. no. 1969. https://doi.org/10.3390/s22051969

[4] Jasova, M., Mendicino, C., & Supera, D. (2021). Policy uncertainty, lender of last resort, and the real economy. *Journal of Monetary Economics forthcoming, 118,* 381–398. https://doi.org/10.1016/j.jmoneco.2020.12.001

[5] Hodula, M. (2022). Does Fintech credit substitute for traditional credit? Evidence from 78 countries. *Finance Research Letters, 46,* part B, art. no. 102469. https://doi.org/10.1016/j.frl.2021.102469

[6] Levytska, S., Pershko, L., Akimova, L., Akimov, O., Havrilenko, K., & Kucherovskii, O. (2022). A risk-oriented approach in the system of internal auditing of the subjects of financial monitoring. *International Journal of Applied Economics, Finance and Accounting, 14*(2), 194–206. https://doi.org/10.33094/ijaefa.v14i2.715

[7] Anand, K., Duley, C., & Gai, P. (2022). Cybersecurity and Financial Stability. *Deutsche Bundesbank Discussion*, 08/2022. https://doi.org/10.2139/ssrn.4073158

[8] Buchak, G., Matvos, G., Piskorski, T., & Seru, A. (2018). Fintech, regulatory arbitrage, and the rise of shadow banks. *Journal of Financial Economics, 130*(3), 453–483. https://doi.org/10.1016/j.jfineco.2018.03.011

[9] Nikonenko, U., Shtets, T., Kalinin, A., Dorosh, I., & Sokolik, L. (2022). Assessing the policy of attracting investments in the main sectors of the economy in the context of introducing aspects of Industry 4.0. *International Journal of Sustainable Development and Planning, 17*(2), 497–505. https://doi.org/10.18280/ijsdp.170214

[10] Melnyk, D. S., Parfylo, O. A., Butenko, O. V., Tykhonova, O. V., & Zarosylo, V. O. (2022). Practice of the member states of the European Union in the field of anti-corruption regulation. *Journal of Financial Crime, 29*(3), 853–863. https://doi.org/10.1108/JFC-03-2021-0050

[11] Kotidis, A., & Schreft, S. (2022). *Cyberattacks and Financial Stability: Evidence from a Natural Experiment. Finance and Economics Discussion Series 2022–2025.* Washington: Board of Governors of the Federal Reserve System. https://doi.org/10.17016/FEDS.2022.025

[12] Cerasi, V., Deininger, S., Gambacorta, L., & Oliviero, T. (2020). How post-crisis regulation has affected bank CEO compensation. *Journal of International Money and Finance, 104,* art. no. 102153. https://doi.org/10.1016/j.jimonfin.2020.102153

[13] Sumets, A., Kniaz, S., Heorhiadi, N., Skrynkovskyy, R., & Matsuk, V. (2022). Methodological toolkit for assessing the level of stability of agricultural enterprises. *Agricultural and Resource Economics, 8*(1), 235–255. https://doi.org/10.51599/are.2022.08.01.12

[14] Novak, A., Pravdyvets, O., Chornyi, O., Sumbaieva, L., Akimova, L., & Akimov, O. (2022). Financial and economic security in the field of financial markets at the stage of european integration. *International Journal of Professional Business Review, 7*(5), art. no. e0835. https://doi.org/10.26668/businessreview/2022.v7i5.e835

[15] Pekkola, S., & Päivärinta, T. (2018). Introduction to the Minitrack on Information Systems Success and Benefits Realization. In: *Proceedings of the 50th Hawaii International Conference on System Sciences*. (p. 4782). Hawaii, USA. https://doi.org/10.24251/HICSS.2018.601

[16] Atstaja, D., Koval, V., Grasis, J., Kalina, I., Kryshtal, H., & Mikhno, I. (2022). Sharing model in circular economy towards rational use in sustainable production. *Energies, 15*(3), art. no. 939. https://doi.org/10.3390/en15030939

[17] Britchenko, I., & Saienko, V. (2017). The perception movement economy of Ukraine to business. *Economic Studies journal, 26*(4), 163–181.

[18] Ceylan, I. E. (2021). The impact of firm-specific and macroeconomic factors on financial distress risk: A case study from Turkey. *Universal Journal of Accounting and Finance*, 9(3), 506–517. https://doi.org/10.13189/ujaf.2021.090325

[19] Böhme, R., Laube, S., & Riek, M. (2017). A Fundamental Approach to Cyber Risk Analysis. *Variance Journal, 12*(2), 161–185. https://www.casact.org/sites/default/files/2021-07/Approach-Cyber-Risk-Bohme-Laube-Riek.pdf

[20] Kou, G., Olgu Akdeniz, Ö., Dinçer, H., & Yüksel, S. (2021). Fintech investments in European banks: a hybrid IT2 fuzzy multidimensional decision-making approach. *Financial Innovation, 7,* art. no. 39. https://doi.org/10.1186/s40854-021-00256-y

[21] Ruiz, P., & Weber, O. (2021). The impact of financial sector sustainability guidelines and regulations on the financial stability of South American banks. *ACRN Journal of Finance and Risk Perspectives, 10*(1), 111–127. https://doi.org/10.35944/jofrp.2021.10.1.007

[22] Hu, D., Zhao, S., & Yang, F. (2022). Will fintech development increase commercial banks' risk-taking? Evidence from China. *Electronic Commerce Research, 24,* 37–67. https://doi.org/10.1007/s10660-022-09538-8

[23] Hooks, D., Davis, Z., Agrawal, V., & Li, Z. (2022). Exploring factors influencing technology adoption rate at the macro level: A predictive model. *Technology in Society, 68,* art. no. 101826. https://doi.org/10.1016/j.techsoc.2021.101826

[24] Borodina, O., Kryshtal, H., Hakova, M., Neboha, T., Olczak, P., & Koval, V. (2022). A conceptual analytical model for the decentralized energy-efficiency management of the national economy. *Polityka Energetyczna, 25*(1), 5–22. https://doi.org/10.33223/epj/147017

[25] Chen, X., Hu, X., & Ben, S. (2021). How do reputation, structure design, and FinTech ecosystem affect the net cash inflow of P2P lending platforms? Evidence from China. *Electronic Commerce Research, 21,* 1055–1082. https://doi.org/10.1007/s10660-020-09400-9

[26] Khan, A., Mubarik, M., & Naghavi, N. (2021). What matters for financial inclusions? Evidence from emerging economy. *International Journal of Finance and Economics, 28*(1), 821–838. https://doi.org/10.1002/ijfe.2451