The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION

OCTOBER 2023

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 140 **NUMBER 9** **October 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:
Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call or email:
Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call
Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISSN: 0005-5506 (Print)
Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub.4815)

Editor-in-Chief, Editor & Board of Editors

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

Cybersecurity of the Banking Sector in the Context of Digitalization of the World's Economy

By Natalia V. Trusova, Iryna O. Chkan, Nataliia M. Kondratska, Natalia Yu. Zakharova and Svitlana O. Osypenko*

The banking sector is an indisputable participant in digitalization processes, as it ensures the process of carrying out financial transactions. Cybersecurity of the banking sector is becoming an extremely relevant and priority element of countries' national security. The purpose of this article is to develop methodological provisions and use in practice the Integral Index of Digital Cyber Security of the banking sector as a qualitative indicator of cyberattack prevention in the dynamic digital space of payment systems regulated by regulators at the macro level. A methodology for calculating the Integral Index of Digital Cyber Security of the banking sector of the economy has been developed, which is used as an indicator and which summarizes, on the one hand, the characteristics inherent in the digital capacity and information security of banking institutions regarding their ability to prevent threats of cyberattacks and dynamically develop in the digital space, and, on the other hand, characteristics that embody the institutional development of the banking sector of a country's economy, which is ensured by the regulators at the macro level.

The continuous strengthening of the demands of society and the needs of business leads to the integration of activities and all spheres of life in cyberspace. Relations of various levels both in the banking sector and in the state are impossible today without information and communication technologies in cyberspace, the functioning of which is hindered by a number of threats and dangers. Mechanisms to protect the banking sector from threats of cyber origin are developed at the global level by international institutions, which are included in the national strategy of each state, taking into account the insurance of the consequences of cyberattacks. The spread of Wi-Fi networks, the inclusion of almost everyone on the internet 24/7 makes them vulnerable to the preservation of the privacy of their own data and business.

An inevitable component of the globalization of digital economies is the growth of organized cybercrime for the purpose of money laundering, terrorist

* Natalia V. Trusova and Iryna O. Chkan are affiliated with the Department of Finance, Accounting and Taxation at the Dmytro Motornyi Tavria State Agrotechnological University in Zaporizhzhia, Ukraine. Nataliia M. Kondratska is affiliated with the Department of Finances and Economic Security at the National University of Water and Environmental Engineering in Rivne, Ukraine. Natalia Yu. Zakharova and Svitlana O. Osypenko are affiliated with the Department of Management and Administration at the Bogdan Khmelnitsky Melitopol State Pedagogical University in Zaporizhzhia, Ukraine.

financing, and illegal possession of money. The globalization of markets and financial flows is combined with the phenomenon of their virtualization, which is based on daily technological achievements, the growth of the share of electronic money in payments, internet trading, internet banking, mobile financial services, etc. Digitization of countries' economies increases their competitiveness (Eisenbach et al., 2022; Issina et al., 2022; Laitsou et al., 2020), so it becomes a priority to develop tools not only for reporting on progress in areas, but also for forecasting progress.

Cyberattacks on the banking system have serious negative consequences for the real economy. The banking sector is dependent on the confidentiality, integrity and availability of data for the payment systems it uses and requires reliable information and communication technology systems. Major cyber-incidents have the potential to disrupt the availability of key economic functions, destroy information and destroy trust in the banking system. In the worst case, a cyber-incident can affect the operational systems of the banking sector and interfere with the performance of critical economic functions, provoking financial contagion, which can lead to the destruction of trust in the payment system of the state as a whole.

Even a minor incident in the field of security of payment operations, such as the leakage of confidential data, can cost a banking institution a loss of reputation, which is equivalent to a loss of business. If the banking institution is unable to absorb them, its financial stability will be at risk. In such conditions, the strengthening of cybersecurity measures is a component of financial monitoring of payment operations of the banking sector operating in the global financial space. The nature and scale of risks to which banking and financial institutions are exposed in the conditions of the development of digital technologies are undergoing significant changes. This leads to the transformation of banking business models into a new model of digitalization of the economy, which ensures the emergence of new management and controlling tasks in the field of cybersecurity. In this regard, the problem of transformation of banking management in conditions of digitalization, search for effective mechanisms for its implementation and protection is quite urgent.

The conceptual foundations of state information policy and cybersecurity as its component in modern conditions are detailed (Novytskyi, 2022). Recommendations have been formulated (Bakalynskyi, 2020) regarding the construction of an effective information protection system without taking into account current world and Ukrainian trends. Justifying the effectiveness of digitalization in all spheres of the economy (Trusova et al., 2021a; Forcadell et al., 2019) models of transformation of the business system architecture into an IT system for expanding investment and innovation activities of business entities are

proposed, and the dependent dynamics between the productivity of innovative services and corporate sustainability in the banking sector is proved. The development of the digital economy increases the efficiency of corporate investments, which provides the financial component of the protection of economies and the banking sector in particular (Huo & Wang, 2022). Since cyber threats (Peihani, 2022) are very dynamic and constantly evolving, building cyber resilience requires constant improvement and adaptation in order to reduce compliance with regulatory requirements regarding risk and threat prevention rules. A key aspect in this direction is the adaptive management of cyber risks and the implementation of regulatory tools (Horna et al., 2022), a detailed description of the identification and interpretation of cybersecurity risks of banks, vulnerability and the list of risks during cyberattacks of a banking institution. Research (Shabbir et al., 2022) consists in detecting suspicious transactions in banking cyber-physical systems.

MATERIALS AND METHODS

Approaches to defining the content of the concept of cybersecurity differ on legal and political grounds. The content of cybersecurity in the banking sector is determined by the political system, regulatory framework, and institutional system of each country (Forcadell et al., 2020; Nehrey at al., 2022). In our opinion, the cybersecurity of the banking sector can be defined as measures of a preventive nature of the functioning of the banking system under the conditions of preserving its integrity, confidentiality and accessibility, responding to incidents of internal and external threats in the cyberspace and overcoming them without hindrance. Cybersecurity in banking is related to the protection of the client and his assets, as well as the bank's resources and profits. Cybersecurity incidents can be extremely expensive, time-consuming, and result in fines from regulators or other lawsuits from aggrieved customers.

The cybersecurity of a banking institution in the area of information technology security consists in ensuring the security of information in complex control technological systems of the banking sector with a set of specific processes and security management tools, protection from both individual types of threats or investigations of cyber incidents, to broader ones – the application of configuration and hardening standards security (Doran et al., 2022; Trusova et al., 2021b). The information security of the banking system requires a complex, well-planned, systematic project to improve its protection systems. Such a complex begins with cyber protection, which combines approaches to identifying threats to the functioning of the bank's information systems, starting from technological ones – optimization of the entire IT infrastructure of the bank to possible threats (the security of IT technologies of the banking institution), to the information security of the entire banking sector – working

with the bank's management (understanding all possible risks of cyberattacks, compliance with legal requirements, use of centralized monitoring tools) and with personnel (data confidentiality, qualifications, work with information carriers, functioning of the bank's servers) (Dadoukis et al., 2021; Trofymenko et al., 2019; Roshan & Abdi, 2022).

The cybersecurity of the banking institution itself is entirely dependent on the bank's management bodies and specialists. Losses of data integrity and unauthorized access to the client's data, risks of malfunctioning of the technical system in the information space reduce the trust of clients, society and the state as a whole if the bank is unable to ensure an adequate level of cybersecurity. The cybersecurity architecture of the banking sector includes a complete list of protection elements with a clearly defined cybersecurity management structure (Fig. 1).

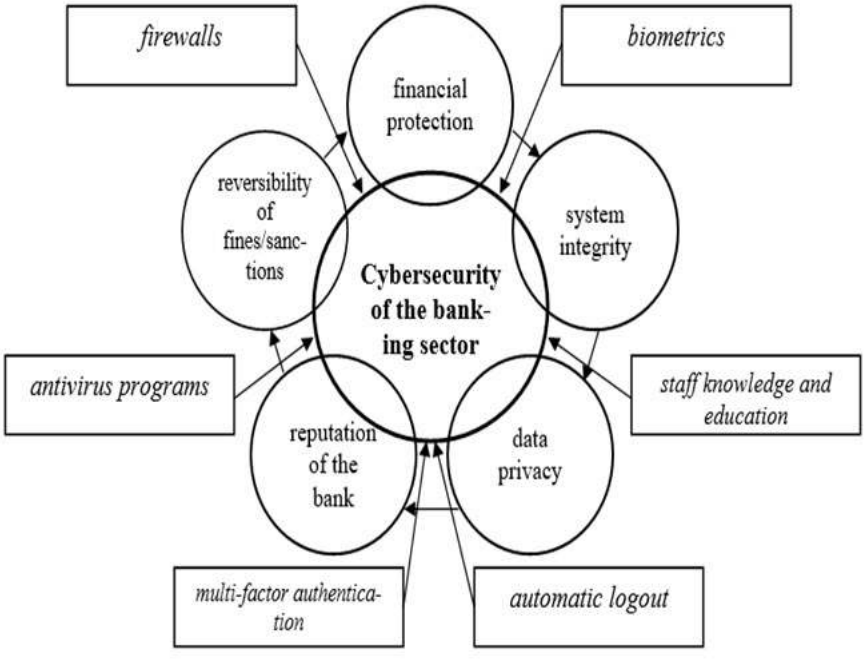

Figure 1. Cybersecurity architecture of the banking sector

Source: Constructed by the authors.

The banking system under the influence of digitization risks primarily depends on cyber risks, which have a direct impact on the entire information system of the state and thus on its security. The digitalization of the banking sector of the economy in the system of protection against cyberattacks strengthens the directions of cybersecurity of banking institutions through

innovation in the modern digital banking environment, using new tools and functions that determine the mutual influence between indicators of institutional and digital capacity of banking institutions as statistically significant and weighty.

This makes it possible to develop a methodology for calculating the integral index of digital cybersecurity of the banking sector of the economy. It will be used as an indicator that summarizes, on the one hand, the characteristics inherent in the digital capability and information security of banking institutions regarding their ability to prevent threats of cyberattacks and dynamically develop in the digital space, and, on the other hand, the characteristics that embody the institutional development of banking sector of the country's economy, which is provided by the regulators of the National Bank at the macro level (Bahuguna et al., 2020; Eisenbach et al., 2022; Kondratska, 2019).

The input data base of the integral indicator of the digital cybersecurity of the banking sector will serve as indicators of the group of digital capacity and information security of banking institutions, i.e. the global index of cybersecurity of the banking sector, the national index of cybersecurity of the banking sector, the index of the development of information and communication technologies of the country, the level of technological readiness of the banking sector and the level of its digital development (National Cyber Security Index, 2020; Lakhno, 2020). Their application will make it possible to evaluate the overall digital cybersecurity system of banking institutions from the point of view of software, technical and information support, as well as the level of countermeasures against external and internal cyber threats.

To form a group of indicators, indicators of the institutional capacity of the banking sector of the economy were chosen according to the data of the World Bank (World Development Indicators, 2022), namely: assessment of corruption control in the economy, assessment of the effectiveness of the financial system of the banking sector, assessment of the quality of regulators of the National Bank, assessment of regulatory requirements for digitalization of banking sectors of the economy, assessment of the stability of payment systems and threats of fraud (cyberattacks). The number of countries and the period are determined by the availability and completeness of data on each of the selected indicators in the database of the World Bank and the E-Governance Academy Foundation (National Cyber Security Index, 2020).

The calculation of the Integral Index of Digital Cyber Security of the banking sector is proposed to be carried out according to the following methodology.

Stage I. Normalization of the array of input data for the purpose of comparison of indicators of different dimensions and their integration. There

are a lot of normalization methods, but for the first stage, nonlinear normalization was chosen, which more effectively smooths data with different signs and values, which is characteristic of the formed set. This process will follow a formula (1):

$$Q_{ij} = \left(1 + e^{\frac{\bar{y}_j - y_{ij}}{\sigma(y)}} \right)^{-1}, \quad (1)$$

where, Q_{ij} – normalized value j-th component of the Integral Index of Digital Cyber Security of the banking sector of the economy in the section of the i-th country; $\bar{y}_j$ – the average value of the j-th component of the Integral Index of Digital Cyber Security of the banking sector of the economy within the studied list of countries; y_{ij} – the actual value of the j-th component of the Integral Index of Digital Cyber Security of the banking sector of the economy in the section of the i-th country; $\sigma(y_j)$ – mean square deviation of the j-th component of the Integrated Index of Digital Cyber Security of the banking sector of the economy within the studied list of countries.

Stage II. Study of the influence of indicators of digital capacity and information security of banking institutions on each of the selected indicators of institutional capacity of the banking sector of the country's economy in order to determine part of the variation of the Integral Index of Digital Cyber Security of the banking sector of the economy. To determine it, it is suggested at this stage to apply canonical analysis, which, better than regression, will allow to determine the value of variation between sets of variables to assess the degree of influence of one set on another.

Stage III. The construction of an Integral Index of Digital Cyber Security of the banking sector of the economy based on the use of the Harrington-Mencher function allows measuring the effectiveness of any system (Harrington, 1965; Mencher & Zemshman, 1986).

The first step of the third stage is the transformation of the normalized values of the indicators of the statistical base of the study to the dimensionless scale of Harrington's desirability using the formula (2) (Harrington, 1965; Mencher & Zemshman, 1986):

$$D_{ij} = \exp(-\exp(-Q_{ij})), \quad (2)$$

where, Q_{ij}– normalized value of the j-th indicator of the digital cybersecurity index of the banking sector of the economy in the section of the i-th country; D_{ij} – the intermediate value of the j-th indicator of the digital cyber security index of the banking sector of the economy in the section of the i-th country, adjusted to the Harrington-Mencher dimensionless desirability scale. The

second step of the third stage is to visualize D_{ij} the dependence on the actual values in the section of each input indicator in order to further choose the type of Harrington-Mencher transformation curve. The third step in this stage is the formalization of the Harrington-Mencher transformation within the limits chosen in the previous step of the dependence D_{ij} on the actual values in the section of each input indicator. That is, based on the results obtained in the second step; it is possible to obtain curves of six types (formula (3)-(13)). The curve of the first type is a W-shaped, growing, symmetrical curve determined by the formula (3) (Harrington, 1965; Mencher & Zemshman, 1986):

$$D_{ij}^{I} = \exp\times\left(-\exp\times\left(9\times\left(\frac{Q_{ij}-\min_{i} Q_{ij}}{\max_{i} Q_{ij}-\min_{i} Q_{ij}}\right)^{1.927}-2\right)\right), \quad (3)$$

where, $D^{I}/_{ij}$ – the intermediate value of the j-th indicator of the digital cybersecurity index of the banking sector in the section of the i-th country, adjusted to the Harrington-Mencher dimensionless desirability scale; $\min {}^{Q_{ij}}/_{i}$ – the minimum value of the normalized j-th indicator of information security of banking institutions in the section of the i-th country; $\max {}^{Q_{ij}}/_{i}$ – the maximum value of the normalized j-th indicator of information security of banking institutions in the section of the i-th country. The curve of the second type is a W-shaped, growing, asymmetric curve with rapid initial growth, which is determined by the formula (4)-(5)) (Harrington, 1965; Mencher & Zemshman, 1986):

$$D_{ij}^{II} = \exp\times\left(-\exp\times\left(9\times\left(\frac{Q_{ij}-\min_{i} Q_{ij}}{\max_{i} Q_{ij}-\min_{i} Q_{ij}}\right)^{k_{II}}-2\right)\right), \quad (4)$$

$$k_{II} = \frac{In\times\ln\left(2-\ln\times\ln\frac{1}{D_{ij}^{II}}\right)}{\ln\left(y_{ij}^{II}-\min_{i} Q_{ij}\right)-\ln\left(\max_{i} Q_{ij}-\min_{i} Q_{ij}\right)}, \quad (5)$$

where, $D^{II}/_{ij}$, $y^{II}/_{ij}$ – any comparable pair within the same country within the same indicator.

The curve of the third type is a W-shaped, growing, asymmetric curve with a slow initial growth, which is determined by the formula (6)-(7) (Harrington, 1965; Mencher & Zemshman, 1986):

$$D_{ij}^{III} = 1 - \exp\times\left(-\exp\left(-\left(9\times\left(\frac{\max_i Q_{ij} - Q_{ij}}{\max_i Q_{ij} - \min_i Q_{ij}}\right)^{k_{III}} - 2\right)\right)\right), \quad (6)$$

$$k_{III} = \frac{In\times\left(2 - \ln\times\ln\frac{1}{D_{ij}^{III}}\right) - \ln 9}{\ln\left(y_{ij}^{III} - \max_i Q_{ij} -\right) - \ln\left(\max_i Q_{ij} - \min_i Q_{ij}\right)}, \quad (7)$$

where, $D^{III}/_{ij}$, $y^{III}/_{ij}$ – any comparable pair within the same country within the same indicator.

The curve of the fourth type is a W-shaped, descending, symmetrical curve determined by the formula (8)-(9) (Harrington, 1965; Mencher & Zemshman, 1986):

$$D_{ij}^{IV} = \exp\times\left(-\exp\left(-\left(9\times\left(\frac{\max_i Q_{ij} - Q_{ij}}{\max_i Q_{ij} - \min_i Q_{ij}}\right)^{1.927} - 2\right)\right)\right), \quad (8)$$

$$k_{IV} = \frac{In\times\left(2 - \ln\times\ln\frac{1}{D_{ij}^{III}}\right) - \ln 9}{\ln\left(y_{ij}^{IV} - \max_i Q_{ij} -\right) - \ln\left(\max_i Q_{ij} - \min_i Q_{ij}\right)}, \quad (9)$$

where, $D^{IV}/_{ij}$, $y^{IV}/_{ij}$ – any comparable pair within the same country within the same indicator.

The curve of the fifth type is a W-shaped, descending, asymmetric curve with a rapid initial decline, determined by the formula (10)-(11) (Harrington, 1965; Mencher & Zemshman, 1986):

$$D_{ij}^{V} = 1 - \exp\times\left(-\exp\left(-\left(9\times\left(\frac{\max_i Q_{ij} - Q_{ij}}{\max_i Q_{ij} - \min_i Q_{ij}}\right)^{k_V} - 2\right)\right)\right), \quad (10)$$

$$k_V = \frac{In\times\left(2 - \ln\times\ln\frac{1}{1 - D_{ij}^{VI}}\right) - \ln 9}{\ln\left(y_{ij}^{V} - \min_i Q_{ij}\right) - \ln\left(\max_i Q_{ij} - \min_i Q_{ij}\right)}, \quad (11)$$

where, $D^{V}/_{ij}$, $y^{V}/_{ij}$ – any comparable pair within the same country within the same indicator.

The curve of the sixth type is a W-shaped, descending, asymmetric curve with a slow initial decline, determined by the formula (12)-(13) (Harrington, 1965; Mencher & Zemshman, 1986):

$$D_{ij}^{VI} = \exp\left(-\exp\left(-\left(9\times\left(\frac{\max\limits_{i} Q_{ij} - Q_{ij}}{\max\limits_{i} Q_{ij} - \min\limits_{i} Q_{ij}}\right)^{k_{VI}} - 2\right)\right)\right), \tag{12}$$

$$k_{VI} = \frac{In\times\left(2 - \ln\times\ln\frac{1}{1-D_{ij}^{VI}}\right) - \ln 9}{\ln\left(y_{ij}^{VI} - \min\limits_{i} Q_{ij}\right) - \ln\left(\max\limits_{i} Q_{ij} - \min\limits_{i} Q_{ij}\right)}, \tag{13}$$

where, $D^{VI}/_{ij}$, $y^{VI}/_{ij}$ – any comparable pair within the same country within the same indicator.

In the fourth step of the third stage, the Integral Index of Digital Cyber Security of the banking sector of the economy is calculated based on the use of the Harrington-Mencher function, as a geometric mean of derivatives of indicators of digital capacity and information security of banking institutions, as well as indicators of institutional capacity (Harrington, 1965; Mencher & Zemshman, 1986):

$$DCSBS_i = \sqrt[n+m]{\prod_{j=1}^{n} (D_{ij}^{*})^{\frac{W_j}{100}} \times \prod_{j=n+1}^{m} D_{ij}^{*}}, \tag{14}$$

where, $DCSBS_i$ – Integral Index of Digital Cyber Security of the banking sector of the economy for the i-th country; n – the number of indicators of the group of institutional capacity of the banking sector of the country's economy; m – the number of indicators of the group of digital capacity and information security of banking institutions; W_j – the degree of variation of the index of digital cybersecurity of the banking sector of the economy under the influence of the j-th input indicator of the institutional capacity of the banking sector of the country's economy (determined at the second stage); $D^{*}/_{ij}$ – the intermediate value of the j-th indicator of the digital cybersecurity index of the banking sector of the economy in the section of the i-th country, adjusted to the Harrington-Mencher dimensionless desirability scale.

Stage IV. Visualization of calculation results and qualitative interpretation of the digital cybersecurity index of the banking sector of the economy. For this purpose, the following interpretation scores are used (Table 1).

Table 1. Criteria of the Integral Index of Digital Cyber Security of the banking sector of the country's economy

Quality interpretation	Quantitative assessment
Very good	1.00 – 0.80
Good	0.80 – 0.63
Satisfactorily	0.63 – 0.37
Bad	0.37 – 0.20
Very bad	0.20 – 0.00

Source: Developed by authors according to the data of E. Harrington (1965), Eh. Mencher and A. Zemshman (1986).

A key priority for the digitalization of cybersecurity in the banking sector should be to increase the awareness of participants and users of the digital banking system regarding the use of innovative information security tools in order to overcome digital noise in the provision of services, prevent the current landscape of fraud and cyberattacks on managed banking Fintech products and ensure their protection.

RESULTS

According to the U.S. Federal Reserve System, banking institutions are 300 times more likely to be cyberattacked than other industries, underscoring how attractive the sector is to cybercriminals. In addition, the banking sector's cybersecurity challenges in trying to implement cybersecurity mitigation strategies can be difficult due to (Eisenbach at al., 2022): a shortage of cybersecurity personnel, where the number of properly trained professionals is far less than the demand; uninformed employees who have either not received adequate cybersecurity training, or their training is outdated and does not take into account new risks; lack of an appropriate budget for combating cybersecurity threats; weak credentials used by employees, making it easier for hackers to break in; mobile devices and applications used for banking transactions are becoming targets for those who want to exploit them.

In March 2022, the ESRB defined a macroprudential policy for the banking sector of the European Union, according to which the functionality of payment systems of banking institutions should be: resilient to how systemic risks materialize; have flexibility to respond to structural changes in the financial system, as well as to cyber risks and risks related to climate change; part of an integrated structure, contributing to the coordinated regulation of all activities in the financial system and to promote cooperation between authorities at all levels. At the same time, the ability of cyber-incidents to impair the performance of the financial system adds a new dimension to macroprudential policy.

Therefore, additional cyber resilience requirements should be introduced for systemically important institutions in order to ensure proportionality and

reduce the burden on banking institutions that are less protective of their assets and that can focus on strengthening cyber hygiene. In addition, macroprudential supervision should cover third-party providers of information and communication technologies (European Systemic Risk Board, 2022). The practice of protecting the banking institution's resources from cyber threats uses complex solutions from the world's leading developers in the field of information protection Fortinet, Barracuda and Commvault – to protect the bank's valuable corporate data, back up information and, if necessary, restore it with the Backup and Recovery service (Javed et al., 2022; Stanikzai & Shah, 2021).

The Complete Data Protection service will help secure enterprise-level information, and the File StorageOptimization service will optimize file storage to reduce costs and risks when storing data. In order to automatically collect information that is stored in electronic form, including emails, bank documents, etc., you can use the eDiscovery & Compliance service. Protection of corporate mail of banking institutions against malicious software, spam, phishing attacks is provided by the Email Security service; threats of multi-level attacks are stopped by the Next Generation Firewall service; Web Application Firewall protects banking institutions' web applications from malicious traffic.

In particular, the Network Access Control service detects unauthorized users of the corporate network; abnormal behavior of resource users is detected by the User and Entity Behavioral Analytics service. Endpoint Security service is used to protect the end point of the IT infrastructure of banking institutions from known and unknown attacks. Each of these services can be connected separately or together with other services for cybersecurity (Naderi et al., 2022; Hou et al., 2022).

The authors of the study put forward a hypothesis regarding the existence of conditioned interactions between the index of digital cybersecurity of the banking sector and the criteria for effective management of macroeconomic indicators, among which we can highlight "The Global Banking Sector Cyber Security Index – GBSCSI," "National Cyber Security Index banking sector" (The National Banking Sector Cyber Security Index – NBSCSI), "Index of development of information and communication technologies of the country" (ICT Development Index – ICT DI), "The technological readiness level of the banking sector" (The Technological Readiness Banking Sector Level – TRBSL), "Digital Development Banking Sector Level – DDBSL." In our opinion, their application to measure the level of digital cybersecurity of the banking sector is justified, as they correspond to the level of digital capability and information security of banking institutions.

Using the average values of the "Global Banking Sector Cyber Security Index" (GBSCSI) for 2018-2021, a visual analysis map of 159 cranes of the

world was built, according to their geographical location (Fig. 2). Thus, the high level of cybersecurity of the banking sector is characteristic of such countries as the USA (93), Great Britain (93), France (92), Estonia (91), Lithuania (91), Singapore (90), Spain (90), Canada (89), Australia (89), Luxembourg (89), Malaysia (89), Netherlands (89), Norway (89), Japan (88), Mauritius (88), Saudi Arabia (88), South Korea (87), Oman (87), a number of EU countries and China. For most of the countries of South America, a number of countries of Eastern Europe, Ukraine, India, Mongolia, Mexico, this index corresponds to the average value (47) and higher. That is, high GBSCSI values correspond to countries characterized by a high level of economic development. On the other hand, the least developed countries with low indicators of economic development also have a low level of digital capacity and information security of banking institutions.

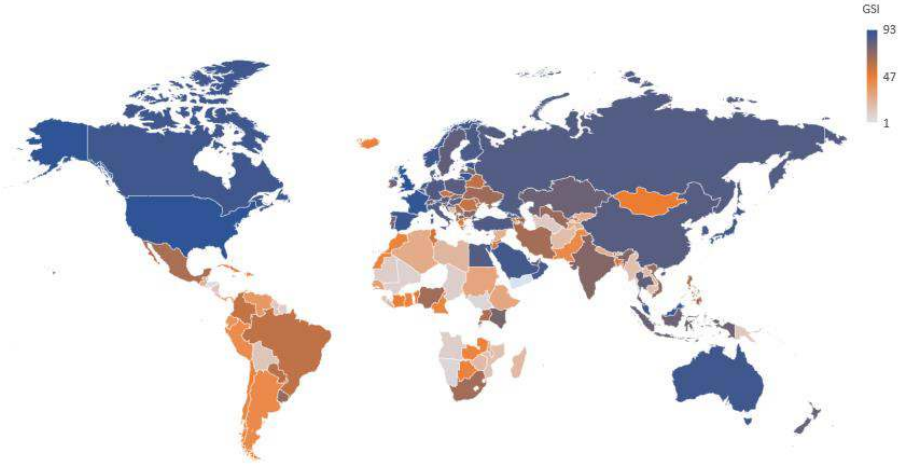

Figure 2. Map of the ranking of countries according to the "Global Banking Sector Cyber Security Index" (GCBSI) on average for 2018-2021

Source: Constructed by the authors according to the data of e-Governance Academe (2022).

The "National Banking Sector Cyber Security Index" (NBSCSI) determines the country's level of preparedness to counter cyber threats and manage cyber-incidents. The results of its determination are used as information for the formation of sources of building national potential in the field of banking cybersecurity. Unlike GBSCSI, the researched NBSCSI takes into account the features of the cyber protection system of Fintech products and payment systems of banking institutions, taking into account national aspects.

For its calculation, 46 indicators are used, combined in 12 directions, namely: development of policy and strategy in the field of cybersecurity; analysis and information on cyber threats; organization of education and professional development in the field of cybersecurity; assessment of contribution to global cybersecurity; level of protection of digital services: responsibility, standards, authorities; organization of protection of basic services; electronic identification and trust services; protection of personal data; responding to cyber incidents; cyber crisis management; fight against cybercrime; military cyber operations (e-Governance Academe, 2022). Using the average empirical values of NBSCSI for 2018-2021, a map was built for visual analysis of 159 countries of the world (Fig. 3).

Thus, developed countries, namely the USA, Canada, Australia, European countries, and others, have high values of the national cybersecurity index of the banking sector. However, when comparing developing countries, for example, Ukraine, which has an index of 64, and Australia with an index of 60, it can be concluded that the level of resistance to cyber threats to Fintech products and payment systems of banking institutions is higher in Ukraine. In addition, this indicator for Ukraine is higher compared to developed countries such as Canada (57), Sweden (57), Norway (62), Japan (62).

This is also typical for Malaysia, India and a number of other developing countries. Countries that are least developed (Tuvalu, South Sudan, Solomon Islands, Congo, Burundi, Turkmenistan, Dominica, Kiribati, Samoa, Belize and several others) have very low NBSCSI values. A comparison of country ratings by the Global Banking Cyber Security Index and the National Banking Cyber Security Indices shows that most countries in the world have above-average ratings for GBSCSI, and the vast majority have average ratings for NBSCSI. That is, it is possible to preliminarily accept our hypothesis regarding the existence of an influence of the level of development of countries on the level of digital cybersecurity of the country's banking sector.

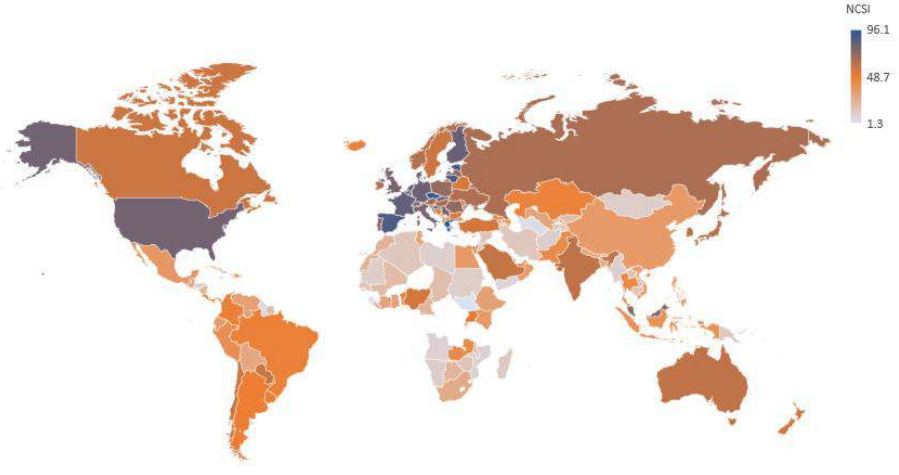

Figure 3. Map of the rating of countries according to the "National Banking Sector Cyber Security Index" (NBSCSI) on average for 2018-2021

Source: Constructed by the authors according to the data of e-Governance Academe (2022).

The main goals of measuring the value of the "Index of development of information and communication technologies of the country" (ICT DI) are to determine the level and evolution over time of ICT in countries; degree of progress in their development; differences between different countries in terms of their ICT development; the potential of their further development (International Telecommunication Union, 2022). It is an integrated indicator that takes into account 11 indicators grouped under three sub-indices: access, use and skills. Using the average empirical ICT DI values for 2018-2021, a map of visual analysis was constructed for 159 countries of the world (Fig. 4).

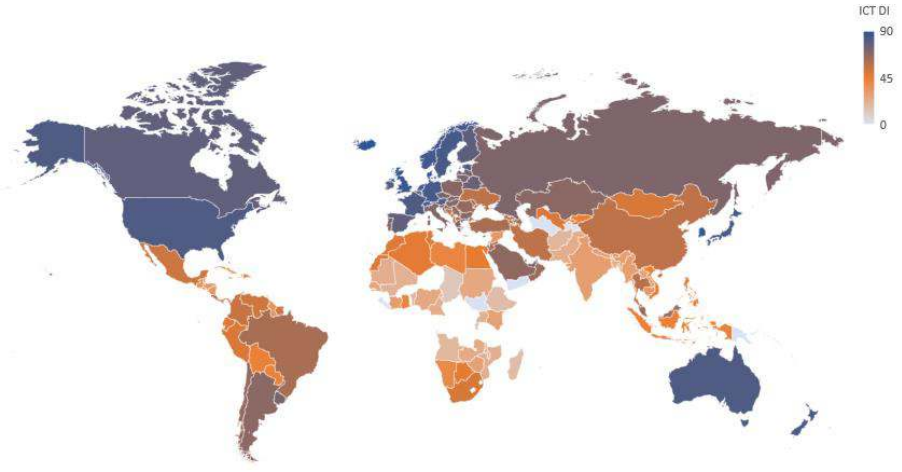

Figure 4. Map of the rating of countries according to the "Index of development of information and communication technologies of the country" (ICT DI) on average for 2018-2021

*Source: Constructed by the authors according to the data of International Telecommunication Union (*2022*).*

According to the analysis, it can be argued that developed countries have high NBSCSI values (Iceland - 90, South Korea - 89, Denmark - 87; Switzerland and Great Britain - 87, Luxembourg, Netherlands and Norway - 85, Germany, Japan and Sweden - 84, New Zealand - 83, Australia, France and USA - 82 and others), the least developed countries correspond to low (Burundi - 15, Chad - 13, Congo - 16, Ethiopia, Haiti, Madagascar and Malawi - 17, Tanzania - 18, Angola and Benin - 19, Afghanistan - 20, Solomon Islands - 21, Uganda, Rwanda, Mali and Kiribati - 22).

Ukraine is in 75th place with a value of 56, at the level of China and Iran, which corresponds to the average level of development of information and communication technologies. Although there is a change in the leaders and outsiders' countries in comparison with the NBSCSI and GBSCSI ratings, the trend regarding the correspondence of the level of economic development of the country to the corresponding indicator of digital capability and information security of banking institutions remains.

The use of the value "The Technological Readiness Banking Sector Level" (TRBSL) allows for a comprehensive assessment of the multifactorial impact of the latest information and communication technologies (ICT DI) on the development of digitalization of the economy, and in particular in the banking sector of individual countries. Its calculation is based on four areas - technology, people, management and influence, which are divided into 12 sub-areas, which

correspond to 62 indicators (e-Governance Academe, 2022; International Telecommunication Union, 2022; Dutta & Lanvin, 2020). Using its average values for 2018-2021, a map was constructed (Fig. 5).

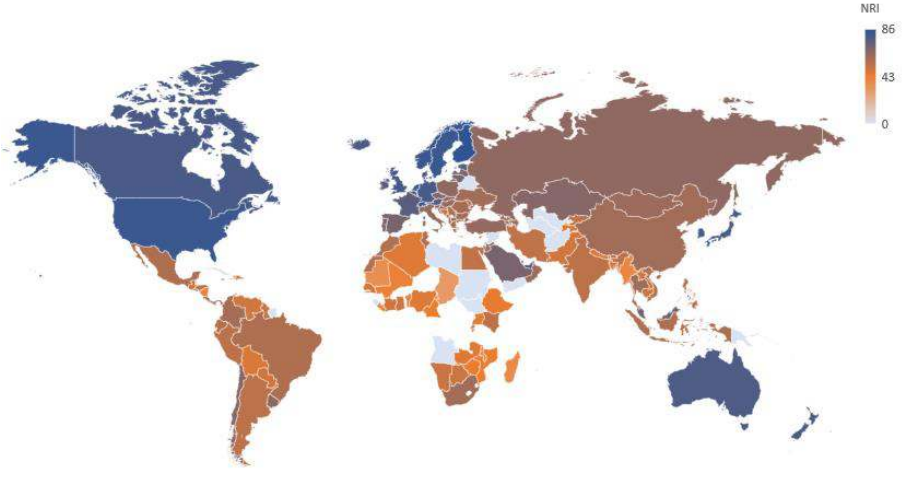

Figure 5. Map of the ranking of countries according to the "The Technological Readiness Banking Sector Level" (TRBSL) on average for 2018-2021

Source: Constructed by the authors according to the data of e-Governance Academe (2022), International Tele-communication Union (2022), S. Dutta and B. Lanvin (2020).

The evaluation of TRBSL average values proves that a high level of technological readiness of the banking sector is characteristic of the following countries: Finland and Singapore – 86, the Netherlands, Norway, Sweden, Switzerland and the USA - 83, Luxembourg and Great Britain – 81, Canada, Denmark, Germany, Japan and South Korea – 80, and others. Countries with a low value are Chad, Burundi, Mauritania, Haiti, Madagascar, Myanmar, Malawi, Nicaragua, Liberia, Tanzania, Mali, Benin and others. In Ukraine, TRBSL is equal to the value of 60, which corresponds to an above average level of technological readiness of banking institutions to conduct Fintech products for the digitalization of banking services in the financial market. It is equal to such countries as China, Jordan, Thailand, and South Africa.

The value "Digital Development Banking Sector Level" (DDBSL) characterizes the level of digital capability and information security of the country's banking institutions and is defined as the average percentage that the country received from the maximum value of the "Index of development of information and communication technologies of the country" and the value of "The Technological Readiness Banking Sector Level." The comparison of countries

according to DDBSL and NBSCSI allows to determine to what extent the degree of digitalization of the banking sector of the country's economy corresponds to its level of digital cybersecurity, which allows for the formation of requirements and the development of regulators of the National Bank regarding the adjustment of the program of digital capability and information security of banking institutions. Using the average empirical values of DDBSL for 2018-2021, a visual analysis map of 159 countries of the world was built (Fig. 6).

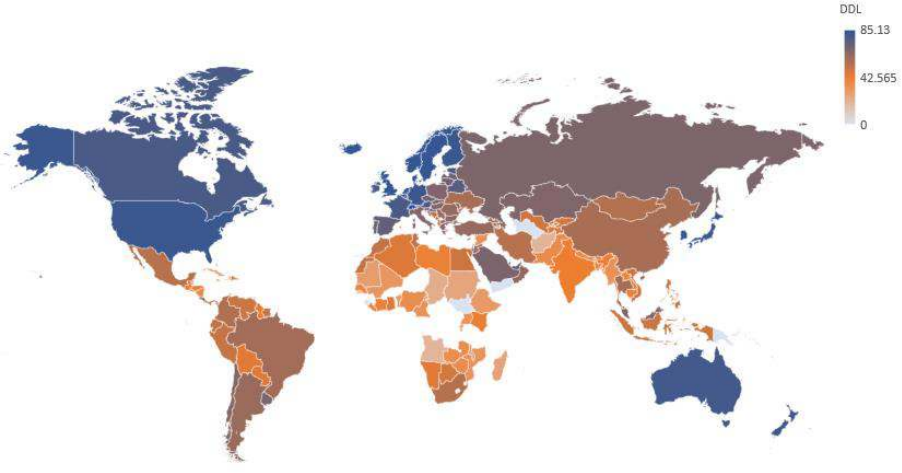

Figure 6. Map of the rating of countries according to the "Digital Development Banking Sector Level" (DDBSL) on average for 2018-2021

Source: Constructed by the authors according to the data of e-Governance Academe (2022), International Tele-communication Union (2022), S. Dutta and B. Lanvin (2020).

The results shown in Figure 6, show that developed countries have a high level of digital development of the banking sector; most of the developing countries have values of the average level and values above the average level; least developed countries – low level. That is, the trends of compliance of the level of digital capability and information security of banking institutions in countries with the level of digital cybersecurity of the banking sector as a whole are maintained.

In general, the values of the above five indicators for Ukraine prove that the country has taken powerful steps to protect payment systems and Fintech products at the macro level during an aggressive cyberattack on the banking sector. This indicates that the country has potential opportunities for the introduction of new innovative and powerful security technologies and the

protection of digital information resources in banking institutions, which are a stimulating driver of the digitalization of the banking sector of the national economy.

DISCUSSION

In 2022, the Ukrainian economy faced unforeseen challenges caused by the full-scale invasion of Ukraine by Russian troops. The banking sector's maintenance of stable work and operational profitability during the current crisis has formed stable business models for banks, taking into account a balanced approach to risks, especially cyber risks. The practice of previous periods hardened the entire financial sector thanks to the close cooperation of all market participants and the systematic work of the regulator. The internet space and electronic platforms of the banking sector have taught how to work effectively, diversifying own portfolios, taking into account interest, market, credit and cyber risks. Thanks to the balanced actions of the regulator, the banking sector has survived and continues to develop, because in the context of accelerated European integration, the planned regulatory and regulatory changes have become urgent.

During 2022, the total number of banks in Ukraine decreased by 4 units (including 2 with Russian capital: Sberbank and Prominvestbank). In addition, despite the difficult situation in the country, it can be stated that there is a traditional tendency in the banking system to reduce the number of banking institutions; taking into account the factor of quick response to maintain stability in stressful conditions (no bank owned by the state or international financial holdings was declared insolvent).

High migration and a decline in business activity in the banking sector have led to a decrease in demand for banking services in certain regions. Thanks to the timely actions of the National Bank and banks to ensure smooth operation, the banking sector of Ukraine passed the first months of the war with moderate losses. As of December 1, 2022 (Fig. 7), the revenue figure of EUR 8,493.0 million maintained its position compared to 2021 – EUR 8,856.40 million despite a significant increase in expenses to EUR 7,980.60 million. This almost equalized income and expenses. However, the banking sector remains operationally profitable and will continue to generate net income (National Bank of Ukraine, 2022).

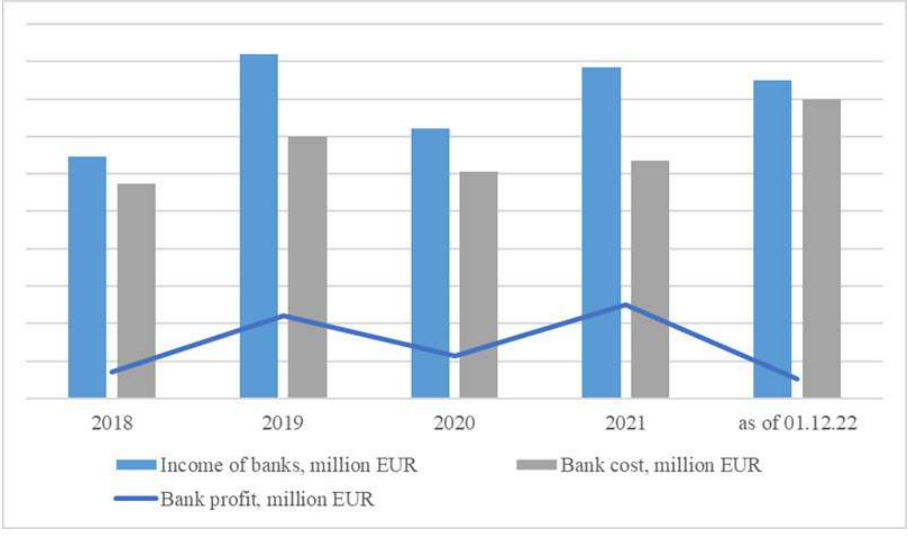

Figure 7. The main indicators of the financial result of banks in Ukraine

Source: Compiled by the authors according to the data of National Bank of Ukraine (2022).

As more payments are made digitally, the risk of cyber-incidents and payment system failures increases. Specialized financial institutions, commercial banks and enterprises create their payment systems based on electronic money, which contain a set of certain rules for conducting payments with electronic money and rules for protection against fraud, appropriate barriers to entering the system, i.e. requirements for authorization and confirmation of payment, software provision and organizations that perform the calculations themselves online. As a rule, the activities of such payment systems are coordinated with central banks or other bodies that regulate payments and settlements on a national or international scale (National Bank of Ukraine, 2022).

Today, more than eighty domestic and international payment systems created by banks and non-banking institutions operate in Ukraine. The National Bank of Ukraine has created two intrastate payment systems: System of Electronic Payments (SEP) and PROSTIR National Payment System. Based on foreign experience, the NBU began to carry out an oversight of payment systems and settlement systems in order to guarantee their continuous and stable functioning (Trusova & Chkan, 2021).

The key links of the Ukrainian payment infrastructure are the System of Electronic Payments (SEP) and the two international payment systems MasterCard and Visa. Despite the full-scale war in Ukraine, payments are made continuously. This is facilitated by the constant, since 2014, strengthening of

NBU requirements to ensure uninterrupted operations in emergency conditions, improvement of cyber protection requirements, as well as harmonized actions of the regulator and the financial community. The number of interbank payments through SEP is gradually increasing along with the recovery of economic activity (Fig. 8). The attempt of external hacker attacks by unknown people from different countries on the information networks of the National Bank on January 14-15, 2022 is indicative.

However, the regulator's information systems worked normally, including the electronic payment system used by banks, the official website and the NBU's internal computer network. IT infrastructure protection is properly organized with the involvement of the NBU Cyber Security Center, other state bodies, banks and financial institutions (Kloba & Kloba, 2022).

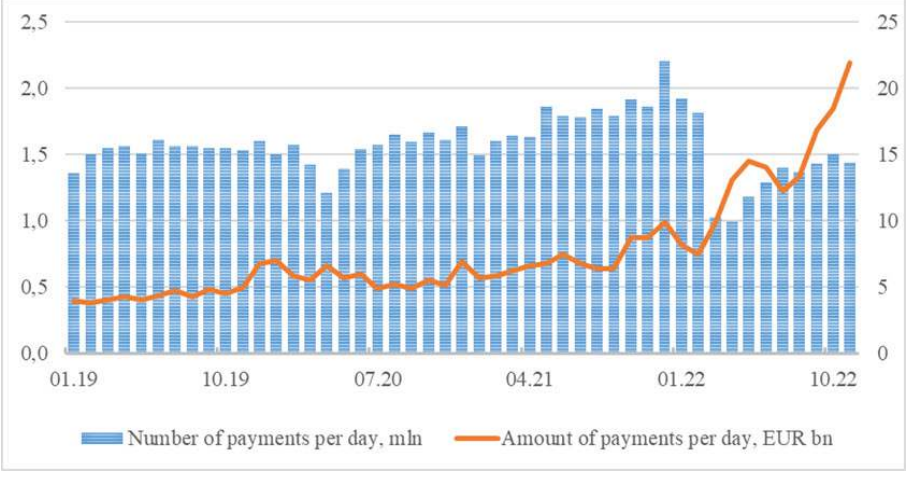

Figure 8. Daily System of Electronic Payments data

Source: Compiled by the authors according to the data of National Bank of Ukraine (2022).

Even in the tensest periods of the war, payments are made on time. The number and amount of transactions with payment cards in October exceeded the pre-war indicators (Fig. 9). The majority of retail transactions carried out using payment cards in Ukraine are served by three payment systems: MasterCard, Visa and PROSTIR. International MasterCard and Visa account for the vast majority of transactions. Their infrastructure is protected from the physical impact of a war in one country, because it is integrated into the international network and has a correspondingly high degree of cybersecurity of payments.

The same applies to online payments using payment cards. Despite the reduction in purchasing activity, in October 2022 the number of transactions

with payment cards issued by Ukrainian banks increased by 3.4% compared to October 2021. The stability of the payment infrastructure reduces the likelihood of a number of risks for the banking system, primarily operational and liquidity risks (National Bank of Ukraine, 2022).

In 2022, numerous attempts of cyberattacks on the banking sector of Ukraine were recorded. The main signs of cyberattacks on the banking sector are numerous DDoS attacks, the active use of phishing emails and malicious blockers. The measures involved by the participants of the banking infrastructure in the prompt updating of software versions consists in conducting penetration testing to identify the problem of the interaction of bank software systems, bottlenecks and quick response to cyberattacks, the use of game theory methods, which will allow considering the IT service from the maximum number of scenarios, because in modern conditions, one-step scripts are rarely used (Kloba & Kloba, 2022).

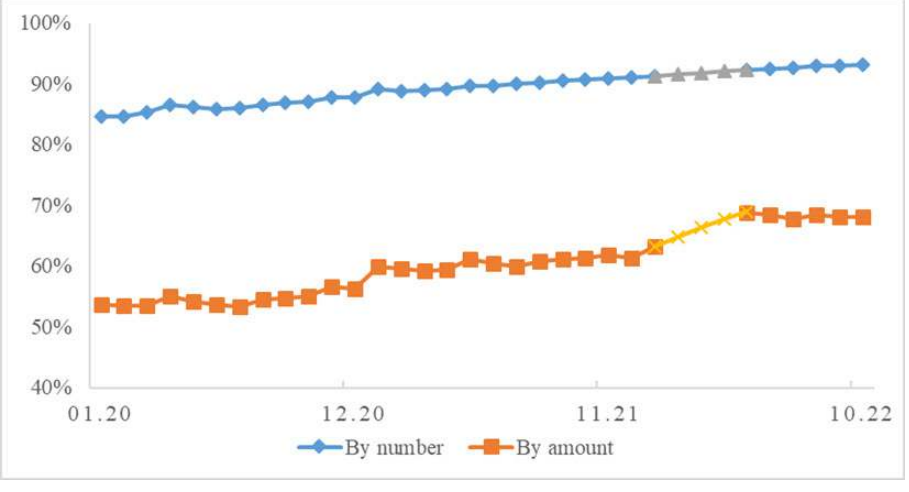

Figure 9. Share of non-cash payments in all card operations, %

Source: Compiled by the authors according to the data of National Bank of Ukraine (2022).

Note: Data provision in February-April 2022 was suspended.

From February 2022, cyberattacks on the banking system of Ukraine were aimed at infrastructure elements (Kloba & Kloba, 2022; Adamyk & Tkachuk, 2019), in particular banking institutions or counterparties that ensured the efficient operation of banks, with the aim of destabilizing the situation in the country: sending fake SMS messages, sending electronic messages between banking institutions about mining buildings and premises, DDoS attacks on the web resources of Ukrainian banks, blocking access to the web resources of

state bodies and institutions by conducting a DDoS attack on DNS servers, fraudulent manipulation of settings autonomous systems at the BGP protocol level.

The priority areas of cybersecurity of the banking sector are the use of preventive information security tools and resources, which, without disturbing the balance of interests between banking institutions and their clients, do not allow disinformation to spread, since the latter is a sign of cyber fraud and a carrier of cyber risks in the financial system of the banking sector of the economy, to forecast which past cyber-incidents must be considered. Therefore, in the current conditions of high vulnerability of the banking sector to cyberattacks, it is necessary to take into account the requirements of international institutions and national regulators regarding the expansion of elements of seamless digitalization of cybersecurity at the international level and at the level of a separate country (Abramova, 2021; Barr et al., 2020; Voronenko et al., 2022).

The authors of the study present a fragment of the used calculation of empirical data regarding the implementation of the methodology for calculating the Integral Index of Digital Cyber Security of the banking sector of the economy from the totality of the studied countries of the world. This made it possible to obtain normalized data for indicators of the institutional capacity of the banking sector of the economy and to conduct a canonical analysis of the interdependence of each of the indicators of digital capacity and information security of banking institutions of different states (Table 2 and Fig. 10).

Thus, according to the "Canonical R" value (Table 2), there is a strong relationship between indicators of digital capability and information security of banking institutions and factors of institutional capability of the banking sector of the economy, and for most factors ($R \geq 0.7$). For "Assessment of stability of payment systems and threats of fraud (cyber-attack)" the relationship is significant, as $0.7 > R \geq 0.5$. Its statistical significance is confirmed by the high value of the Pearson test ("Chi2" column), the significance level of which does not exceed 0.05 ($p = 0.000$). The presented value "Complete redundancy" explains the variability of the indicators of the institutional capacity of the banking sector of the economy. Thus, the indicator "Assessment of the efficiency of the financial system of the banking sector" is transformed when the indicators of digital capacity and information security of banking institutions change, i.e. their variation leads to a change in the efficiency of the financial system of the banking sector by 75.61%.

Table 2. Canonical analysis of indicators of the institutional capacity of the banking sector of the world economy (calculation fragment)

Name of the indicator	Total redundancy	Canonical R	Chi²	p
Assessment of corruption control in the economy	56.39	0.751	128.2	0.000
Evaluating the effectiveness of the financial system of the banking sector	75.61	0.870	218.0	0.000
Quality assessment of the National Bank's regulators	72.17	0.850	197.6	0.000
Assessment of regulatory requirements for digitalization of banking sectors of the economy	59.90	0.774	141.2	0.000
Assessment of the stability of payment systems and threats of fraud (cyberattacks)	35.01	0.592	66.6	0.000

Source: Calculated by the authors.

The change in the normalized values of the indicators of institutional capacity to the dimensionless scale of Harrington-Mencher is presented in Figure 10.

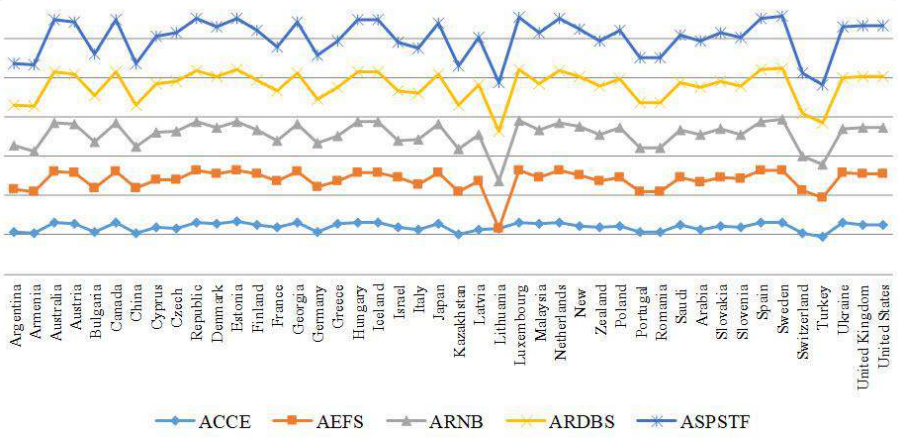

Figure 10. Normalized values of indicators of institutional capacity of the banking sector of the economy of the countries of the world, reduced to the dimensionless Harrington-Mencher scale (calculation fragment for 41 countries of the world)

Source: Compiled by the authors according to the data of e-Governance Academe (2022), International Tele-communication Union (2022), S. Dutta and B. Lanvin (2020).

Note: ACCE – Assessment of corruption control in the economy; AEFS – Assessment of the efficiency of the financial system of the banking sector; ARNB – Assessment of the quality of regulators of the National Bank; ARDBS – Assessment of regulatory requirements for digitization of the banking sector of the economy; ASPSTF – Assessment of stability of payment systems and threats of fraud (cyberattacks).

Since the factors of the institutional capacity of the banking sector of the economy have a direct impact on the level of digital capacity and information

security of banking institutions, the obtained variability values allow us to use them as a weighting effect of indicators when calculating the Integral Index of Digital Cyber Security of the banking sector of the country's economy. A scatter diagram of the canonical values for the first pair of canonical roots was constructed (Figure 11), in which the horizontal axis is the components of the digital capacity and information security of banking institutions, and the vertical axis is the indicator of the institutional capacity of the banking sector of the economy of the studied 159 countries of the world.

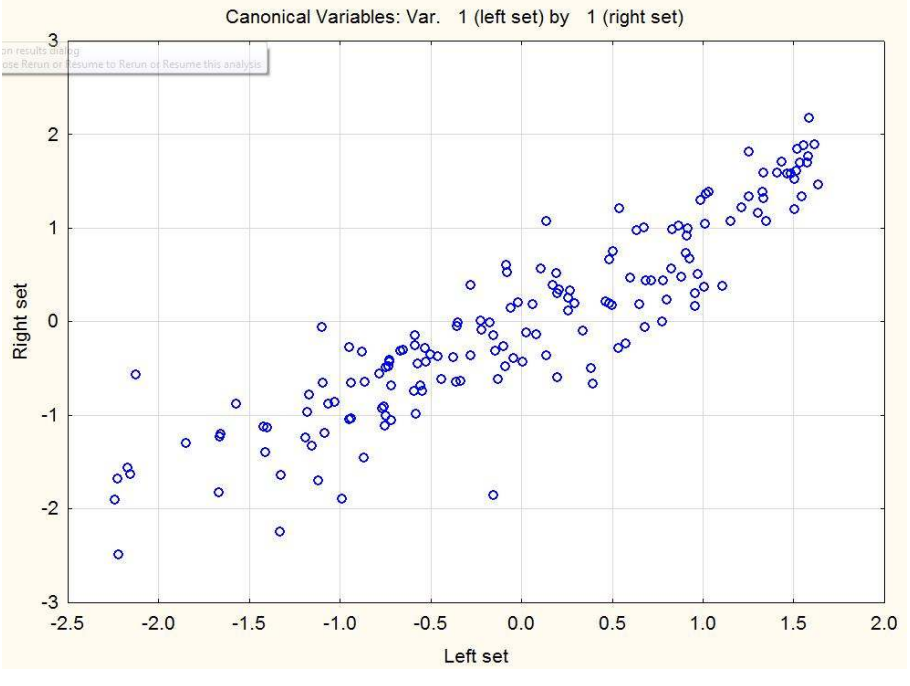

Figure 11. Scatter diagram of canonical values of indicators of digital capacity and information security of banking institutions, as well as indicators of institutional capacity of the banking sector of the economy of 159 countries of the world

Source: Developed by the authors.

According to Figure 11, the clustering of observations is characteristic of linear dependence, while the graph does not contain significant deviations, except for two, which is possibly due to the different rates of development of digital capacity and information security of banking institutions in countries and the institutional capacity of the banking sector for some countries. In general, the obtained values in the diagram demonstrate that there is a fairly close relationship between the indices of the institutional capacity of the

banking sector of the economy, as well as the digital capacity and information security of banking institutions. The calculated values of the canonical levers made it possible to determine the regression equation (formula (15)) for the canonical variables of the left and right sets:

$$\begin{aligned} Y(1\,root) &= 0.3247y_1 + 0.2687y_2 + 0.2344y_3 + 0.2127y_4 + 0.1346y_5 \\ Y(2\,root) &= 1.2642x_1 + 0.3998x_2 - 0.3492x_3 - 0.2377x_4 - 0.1144x_5 \end{aligned}, \quad (15)$$

For each component of the Integral Index of Digital Cyber Security of the banking sector of the economy, a graph was constructed, the analysis of the shape of which made it possible to determine the type of curve. Thus, the curve of the second type is characteristic of the level of Digital Development Banking Sector Level (DDBSL) and the National Banking Sector Cyber Security Index (NBSCSI). An example of the obtained result for NBSCSI in Figure 12.

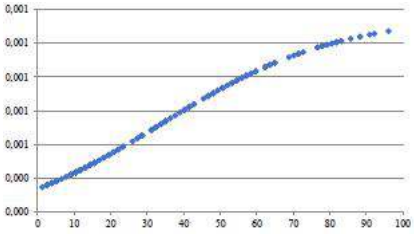

Figure 12. Graph of the curve of the second type for the indicator "National Banking Sector Cyber Security Index" (NBSCSI)

Source: Developed by the authors.

For all other indicators, a curve of the first type was identified, an example of which is given for assessing the quality of the National Bank regulators in Figure 13.

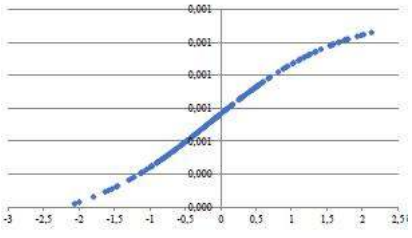

Figure 13. Graph of the curve of the first type for the indicator "Assessment of the Quality of Regulators of the National Bank" (NBSCSI)

Source: Developed by the authors.

According to the results of the calculation, a map of the distribution of countries was built according to the determined Integral Index of Digital Cyber Security of the banking sector of the country's economy (Fig. 14). Five groups

of countries were obtained, in which the possibilities of state control over digital cybersecurity of the banking sector of the economy are identified. Thus, 49 countries were included in the "very good" level of countermeasures against threats: Western, Northern and Southern Europe, the USA, Canada, Australia, Japan, New Zealand, Malaysia, Saudi Arabia, Israel and other countries.

That is, this group was formed by countries that are mostly developed, have a powerful economy, high scientific and technical potential, and use strategic monitoring approaches for the digitalization of the banking sector's cybersecurity at the country level. They have the highest capabilities compared to other countries to resist cyber threats, information fraud and cyberattacks, which lead to a decrease in the state of security of information resources in the country's national payment systems and the personal interests of developers of new innovative technologies for the banking sector, as well as participants and users of Fintech products.

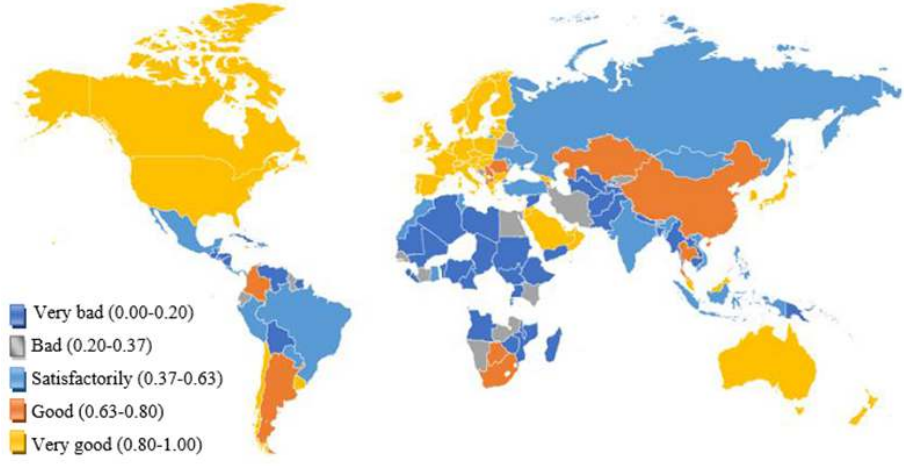

Figure 14. Map of the distribution of countries according to the Integral Index of Digital Cyber Security of the banking sector of the economy

Source: Developed by the authors.

According to calculations, 14 countries of the world were assigned to the group that has a level of digital cybersecurity of the banking sector with a rating of "good." It was formed by a number of newly industrialized countries – Brazil, China, Thailand, and a number of developing countries – Albania, Argentina, Armenia, Kazakhstan, Romania, Serbia and others. Most characteristic of this group are significant deviations for indicators of corruption control and requirements for digitalization of the banking sector of the economy.

That is, the countries of this group need to change the approaches to the development of the National Bank regulators regarding the information security of the country's banking institutions, namely to improve the regulatory requirements for the digitalization of the banking sector of the economy and its cybersecurity, strengthen responsibility for cyber-incidents, and implement standards for the protection of personal data of participants and users of payment systems, to reorganize institutions responsible for information security in the country.

Countries that were classified as "satisfactory" are 24 developing countries: Azerbaijan, Brazil, Moldova, Mongolia, Morocco, Peru, Russian Federation, Tunisia, Ukraine, etc. This group is characterized by the fact that the level of development of information and communication technologies is lower than the average level, since other indicators of digital capacity and information security of banking institutions exceed it. In addition, for this group, the values of indicators of the institutional capacity of the banking sector are critical and for most countries are lower than the sample average.

Unlike the previous group, the countries of the "satisfactory" group should pay attention to the development of a set of strategic measures that will contribute to the development of digital technologies for the information security of payment systems of banking institutions. First of all, these countries need to focus on the measures of the National Bank regulators regarding digital capacity and information security, namely to implement: changes to regulatory documents in the field of information security and information protection, especially in terms of criminal liability for cybercrimes; measures to combat corruption and reduce the level of threats of fraud (cyberattacks). This is especially relevant for such countries as Ukraine, Mexico, Brazil, Azerbaijan, etc. measures to create special units to respond to cybercrimes.

18 countries were included in the "bad" group – Barbados, Belarus, Bhutan, Egypt, Ecuador, Iran, Kenya, Kyrgyzstan, Namibia, Zambia and others, and 54 countries were in the "very bad" group: Afghanistan, Cameroon, Cambodia, Libya, Mozambique, Nicaragua, Nigeria, Sudan, Tajikistan, Turkmenistan, etc. The countries of these groups are characterized by low or very low indicators of the institutional capacity of the banking sector, as well as indicators of digital capacity and information security. Accordingly, the risk of the existence of a threat to the information security of banking institutions for these countries is critical or significantly critical, that is, they are more vulnerable, and their available information resources are not sufficient to overcome the consequences of a cyber-crisis, information fraud or information war.

On the other hand, the risk of them being the target of cyberattacks is small compared to countries in the "very good," "good" and "satisfactory" groups.

Increasing the level of economic development of such countries will significantly affect measures to strengthen the level of digital cyber security of the country's banking sector. Therefore, the cybersecurity of the banking sector in the conditions of the digital economy of the countries of the world takes into account not only separate areas, such as the level of development of information and communication technologies, the degree of digitalization and informatization of payment systems of banking institutions, but also the level of state regulators of the National Bank from the position of ensuring high-quality identification and visualization of distributed regulations, standards and legal aspects of the effective work of banking institutions on information security issues.

The level of digital cybersecurity of the banking sector of developing countries, in particular in Ukraine, has an average possibility of developing the digitalization of the banking sector of the economy, which can provoke threats in the economy, social and political spheres. These countries should reformat not only the strategy of attracting investments in the development of digital security of the banking sector to improve the level of economic development, but also stimulate the improvement of the level of efficiency of the financial system and its security at the national level.

CONCLUSION

Standardization and security of the banking sector of the economy in the global space is undoubtedly a priority issue of the modern society. Along with this, opportunities to ensure the free movement of money, the source of which are illegal financial transactions, fraud and other actions, are increasing. The illegal circulation of funds and the financing of organized crime are becoming the main problems that threaten the economy of any country. At the same time, the financial system of the banking sector takes a rather active part in this, as it provides the process that leads to the legalization of such financial transactions. The cybersecurity of the banking sector plays not the last role, since the ability of financial institutions to prevent obstacles to transactions with funds obtained from illegal sources depends on the level of its organization and compliance with international standards. It can be said that the high level of digital cybersecurity in payment systems, which have reliable innovative information encryption modules, reduce the risks of fraud when using transactions in banking institutions in order to prevent those that are illegal.

The international financial and economic community should develop measures aimed at determining the relationship between the economy, politics and cybersecurity of the banking sector in order to neutralize organized cyberattacks aggressively directed at financial flows. In addition, these actions must go beyond the borders of one country in order to track and block illegal

financial flows wherever they are hidden. In addition, it is impossible to painlessly overcome the consequences of information wars, since they are able to penetrate into all spheres of life in society and exert extremely negative pressure on humanity. The losing party in the information war may lose control, become subject to the aggressor country, face the destruction of the economic system, disruption of political stability, destruction of structures unnecessary to the winner, and even the national security system. However, the consequences in the banking sector are particularly noticeable, since the object of cybercrimes is often financial information, the loss of which can lead to financial losses in the country's economy. Accordingly, the issue of protection against such weapons should be one of the highest priorities for national and global cybersecurity systems.

REFERENCES

Abramova, A. (2021). The risk system of commercial banks in conditions of digitalization. *Problems and Prospects of Management Economics, 4*(28), 186-193.

Adamyk, B., & Tkachuk, V. (2019). Payment systems: fundamental principles and prospects for transformation. *Economic Analysis, 29*(3), 63-73.

Bahuguna, A., Bisht, R.K., & Pande, J. (2020). Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal*, *29*(5), 250-266.

Bakalynskyi, O. (2020). Model and methods for determining the design characteristics of information security management systems. Retrieved from https://www.researchgate.net/publication/348788054_Model_ta_metodi_viznacenna_proektnih_harakteristik_sistem_upravlinna_informacijnou_bezpekou_Monografia

Barr, M.S., Harris, A., Menand, L., & Xu, W. (2020). Building the payment system of the future: how central banks can improve payments to enhance financial inclusion. *Center on Finance, Law & Policy,* 1-28.

Dadoukis, A., Fiaschetti, M., & Fusi, G. (2021). IT adoption and bank performance during the Covid-19 pandemic. *Economics Letters*, *204,* 109904.

Doran, N.M., Bădîrcea, R.M., & Manta, A.G. (2022). Digitization and financial performance of banking sectors facing COVID-19 challenges in Central and Eastern European countries. *Electronics (Switzerland), 11*(21), 3483.

Dutta, S., & Lanvin, B. (2020). The Network Readiness Index 2019: Towards a Future-Ready Society. Retrieved from https://networkreadinessindex.org/wp-content/uploads/2020/03/The-Network-Readiness-Index-2019-New-version-March-2020.pdf

Eisenbach, T.M., Kovner, A., & Lee, M.J. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*, *145*(3), 802-826.

European Systemic Risk Board. (2022). Retrieved from https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr221208~a1fb778a2d.en.html

Forcadell, F.J., Aracil, E., & Úbeda, F. (2019). The influence of innovation on corporate sustainability in the international banking industry. *Sustainability (Switzerland), 11*(11). https://doi.org/10.3390/su11113210

Forcadell, F.J., Aracil, E., & Úbeda, F. (2020). The Impact of corporate sustainability and digitalization on international banks' performance. *Global Policy*, *11*(S1), 18-27.

Harrington, E. (1965). The desirability function. *Industrial Quality Control*, *21*(10), 494-498.

Horna, C. J., Toro, L., & Regalado-Pezua, O. (2022). Silverbank: Vulnerability and risks duringcy be attacks. *Emerald Emerging Markets Case Studies*, *12*(1), 1-33.

Hou, L., Li, Y., Luo, W., & Sun H. (2022). Adaptive tracking control of switched cyber-physical systems with cyberattacks. *Applied Mathematics and Computation, 415,* https://doi.org/10.1016/j.amc.2021.126721

Huo, P., & Wang, L. (2022). Digital economy and business investment efficiency: Inhibiting or facilitating? *Research in International Business and Finance*, *63*. https://doi.org/10.1016/j.ribaf.2022.101797

International Telecommunication Union. (2022). The ICT Development Index (IDI): conceptual framework and methodology. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2016/methodology.aspx

Issina, B., Bekzhanova, S., Ananiev, S., & Kenzhekeeva A. (2022). Prospects for the development of digital economy in the Republic of Kazakhstan. *AIP Conference Proceedings 2449*, 040001. https://doi.org/10.1063/5.0103817

Javed, A., Lakoju, M., Burnap, P., & Rana, O. (2022). Security analytics for real-time for ecasting of cyber-attacks. *Software-Practice and Experience*, 52(3), 788-804.

Kloba, L., & Kloba, T. (2022). Cyber threats of the banking sector in the conditions of the war in Ukraine. *Financial and Credit Activity Problems of Theory and Practice*, *5*(46), 19-28.

Kondratska, N. M. (2019). Financial and economic security of banking institutions: threats and ways to overcome them. *Bulletin of the National University of Water Management and Nature Management. Economic Sciences, 4*, 48-60.

Laitsou, E., Kargas, A., & Varoutas D. (2020). Digital competitiveness in the European Union era: The Greek case. *Economies, 8*(4), 85.

Lakhno, V.A. (2020). Algorithms for forming a knowledge base for decision support systems in cybersecurity tasks. *Advances in Intelligent Systems and Computing*, *938*, 268-278.

Mencher, Eh. M., & Zemshman, A. Ja. (1986). *Basics of planning an experiment with elements of mathematical statistics in a study on viticulture.* Kishinev: Shtiintsa.

Naderi, E., Pazouki, S., & Asrari, A. (2022). A remedial action scheme against false data injection cyber-attack sin smart transmission systems: Application of thy ristor-controlled series capacitor (TCSC). *IEEE Transaction son Industrial Informatics, 18*(4), 2297-2309.

National Bank of Ukraine. (2022). Financial Stability Report. https://bank.gov.ua/admin_uploads/article/FSR_2022-H2.pdf?v=4

National Cyber Security Index (NCSI). (2020). E-Governance Academy Foundation. Retrieved from https://ncsi.ega.ee/ncsi-index/

e-Governance Academe. (2022). National Cyber Security Index. Retrieved from https://ncsi.ega.ee/ncsi-index/

Nehrey, M., Voronenko, I., & Salem, A.-B. M. (2022). Cybersecurity Assessment: World and Ukrainian experience. In *2022 12th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 335-340), Slovakia: Ruzomberok.

Novytskyi, V. (2022). Strategic principles of ensuring information security in modern conditions. *Information and Law, 1*(40), 111-118.

Peihani, M. (2022). Regulation of cyber risk in the banking system: A canadian case study. *Journal of Financial Regulation, 8*(2), 139-161.

Roshan, Y.E., & Abdi, Y. (2022). ICT and Information Asymmetry; New Evidence of the Financial System in Selected MENA Countries. *Iranian Economic Review, 26*(2), 445-458.

Shabbir, A., Shabir, M., Javed, A. R., Chakraborty, C., & Rizwan, M. (2022). Suspicious trans action detection in banking cyber-physical systems. *Computers and Electrical Engineering, 97*. https://doi.org/10.1016/j.compeleceng.2021.107596

Stanikzai, A. Q., & Shah, M. A. (2021). Evaluation of cyber security threats in banking systems. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-4), USA: Orlando, FL.

Trofymenko, O., Prokop, Y., Loginova, N., & Zadereyko, O. (2019). Cybersecurity of Ukraine: analysis of the currentstate. *Information Protection, 21,* 3.

Trusova, N.V., & Chkan, I. O. (2021). Payment systems in Ukraine and the risks of their operation. *Business Inform, 1,* 257-263.

Trusova, N.V., Melnyk, L.V., Shilo, Z.S., & Prystemskyi, O.S. (2021a). Credit-investment activity of banks of the Ukraine: Financial globalization, risks, stabilization. *Universal Journal of Accounting and Finance, 9*(3), 450-468.

Trusova, N.V., Yeremenko, D.V., Karman, S.V., Kolokolchykova, I.V., & Skrynyk, S.V. (2021b). Digitalization of investment-innovative activities of the trade business entities in network IT-system. *Estudios de Economia Aplicada*, *39*(5), 1-19.

Voronenko, I., Klymenko, N., & Nahorna, O. (2022). Challenges to Ukraine's innovative development in a digital environment. *Management and Production Engineering Review, 13*(4), 48-58.

World Development Indicators. (2022). The World Bank. https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on.