DOI: 10.55643/fcaptp.3.62.2025.4702

Yuliia Biliavska
Candidate of Economy Sciences, Associate Professor of the Department of Management, State University of Trade and Economics, Kyiv, Ukraine;
e-mail: y.biliavska@knute.edu.ua
ORCID: 0000-0002-8183-4036
(Corresponding author)

Valentyn Biliavskyi
Candidate of Economy Sciences, Associate Professor of the Department of Management of Foreign Economic Activity of Enterprises, State University "Kyiv Aviation Institute", Kyiv, Ukraine;
ORCID: 0000-0003-2129-1524

Yaroslav Shestak
PhD in Technical Sciences, Senior Lecturer of the Department of Software Engineering and Cybersecurity; Director of the Information and Computing Center of the Main Center of Information Technologies, State University of Trade and Economics, Kyiv, Ukraine;
ORCID: 0000-0002-5102-9642

Nataliya Dyeyeva
D.Sc. in Economics, Professor of the Department of Management, State University of Trade and Economics, Kyiv, Ukraine;
ORCID: 0000-0002-2278-549X

Maksym Kolesnyk
Candidate of Economy Sciences, Associate Professor of the Department of Management of Foreign Economic Activity of Enterprises, State University "Kyiv Aviation Institute", Kyiv, Ukraine;
ORCID: 0000-0003-0814-4220

Andrii Tryvailo
Candidate of Economy Sciences, Associate Professor of the Department of Industrial Marketing, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine;
ORCID: 0009-0006-3059-5780

Received: 21/01/2025
Accepted: 18/05/2025
Published: 30/06/2025

MONITORING OF CYBER RISKS IN THE FINANCIAL SECTOR OF THE ECONOMY

ABSTRACT

The financial sector of the economy is an attractive target for cyber-attacks because it plays an important role in intermediating the movement of funds. The article is devoted to monitoring cyber risks that may affect the functioning of electronic services. It is established that in the practical sphere, cyber-attacks are growing exponentially every year, but in the scientific sphere, considerable attention is paid to the identified issues, namely, cyber risks. In today's market environment, the communication architecture is based on the fact that financial institutions are critical to global commercial activities, as well as operations at the local, national and international levels of economic activity. The key objective of the study was to identify, classify and monitor cyber risks caused by both internal and external cyber threats in the financial sector.

The study found that cyber risks for the financial sector mainly relate to the leakage of customer data or certain corporate information, financial losses, forced interruptions in the operation of electronic services, and ultimately the loss of reputational capital and mutual trust. During the bibliometric analysis, the author identified scientific papers that characterise the essence, systematise methodological tools, study classifications of cyber risks in the context of financial activities, and identify opportunities to overcome them in order to ensure cyber resilience. An original matrix of the relationship between the identified scientific clusters and cyber risks in the financial sector is proposed, which will allow us to focus on the development of promising solutions to overcome them.

Financial sector institutions are in constant need of developing recommendations for protection against the negative impact of cyber risks, as they still use outdated electronic systems that are not resistant to the threats of possible cyber attacks. The conclusions confirm the relevance and importance of dealing with cyber risks in the financial sector to ensure stability and increase confidence in electronic services.

Keywords: risk, management, bibliometric analysis, cybersecurity, cyber fraud, cyber criminals, clusters, communication infrastructure, digital technologies

JEL Classification: D83, G30, G32

INTRODUCTION

At the current stage of development, globalization processes have contributed to the rapid entry of digital reality into human life. Mobile devices, social networks, navigation systems, payment resources and search engines, and cloud computing capabilities are massively and constantly enabled, confirming the fact that digital transformation is a key trend in civil society. That is why cybersecurity has long ceased to be a problem exclusively for information technology professionals (Von and Niekerk, 2013; Mishna et al., 2012; Knowles et al., 2015). Cybersecurity incidents in the financial environment usually affect the activities of top management, but consumers have long been aware of the consequences of cyber threats. Reports of information security threats are increasingly becoming commonplace and need to be addressed effectively.

More than a third of incidents in the financial sector are related to the exploitation and management of vulnerabilities. They are used by hackers at all stages of cyberattack development, during attempts to hack into the victim's web resources, applications and services, during horizontal network penetration, during attempts to compromise financial systems within the communication infrastructure, and form cyber risks.

Therefore, regular patch management and a well-established vulnerability management process remain the basis for building a secure communications infrastructure. In addition, more and more incidents and cyber risks occur due to unauthorized access to systems and services. In the context of the banking sector, this includes, for example, components of the automated banking system and remote banking services, as well as internal document management systems and key databases. Risk management professionals are at a critical juncture. Today, businesses are rapidly adopting digital technologies in an environment where the amount of data is constantly increasing, the level of automation is rising, cyberattacks are becoming more sophisticated, and customer expectations are constantly growing and changing (Abawajy, 2014). While many technological risks have long been known, the danger of vulnerability has increased as the adoption of digital technologies increases risks not related to technology per se. Given the expanded range of new threats, the study of cyber risks and the development of the main trends to overcome them in the financial sector of centralized and decentralized governance is becoming increasingly important.

LITERATURE REVIEW

In the literature review, we will consider in more detail the studies that are to some extent related to cyber risks in the financial sector and the business environment. For example, Eling et al. (2021) emphasize that the study of cybersecurity includes both technical and economic or managerial aspects. The key conclusions are that cyber risks are not included in the main risks of enterprises, and to overcome them, it is necessary to ensure the cyber resilience of the enterprise. In turn, Rahman et al. (2024) propose an updated IT infrastructure based on artificial intelligence, supported by blockchain technology and designed to optimize risk management processes in the organizational environment. Implementation of such a system is a significant solution for improving organizational cybersecurity. However, the authors do not identify the disadvantages and risks that may be provoked by the use of such technologies.

Rampášek et al. (2025) examines the impact of the cybersecurity strategy declared by the European Commission. The authors prove that artificial intelligence technology, products, and services should be cyber secure through a high level of standardisation. The development and adoption of technical standards will help to formulate criteria for assessing the conformity of modern information technologies. We share the authors' opinion on the importance of special standardisation of artificial intelligence and further certification of digital products and services designed to ensure cyber resilience in Europe.

On the other hand, Panetta and Leo (2024) are convinced that digitalisation in the financial sector is under the overarching threat of systemic cyber risks. Such risks are a potential opportunity for cyberattacks to cause large-scale disruptions in the financial system. That is why, according to the authors, ongoing network analysis and study of cyber threats can be a valuable tool for avoiding vulnerabilities in financial systems. Rees et al. (2011) found that it is possible to reduce asset losses from cyberattacks by implementing security countermeasures that help protect privacy. The drawback of the presented studies is the lack of methods that allow identifying and assessing cyber risks. Such approaches will help to save resources and timely anticipate the emergence of cyber risks in the economic financial sector, where a large number of customers are active participants.

An interesting paper is Birindelli and Iannuzzi (2024), where the authors analyse cyber risk with particular reference to the banking and financial sector using scientific approaches and practical solutions. Cremer et al. (2022) also analyses the existing academic and industry literature on cybersecurity and cyber risk management. The study yielded unique results from a dataset of 5219 peer-reviewed cyber studies. According to the authors, the lack of available data on cyber risk poses a serious challenge for stakeholders seeking to address this issue. The resulting assessment and categorisation of data will help cybersecurity researchers and the insurance industry to understand, measure and manage cyber risks. That is why it is important to continue research using a bibliometric review to identify papers that focus on cyber risks in the financial sector.

In turn, Whitty (2019) developed a theoretical framework for predicting susceptibility to becoming a victim of cyber fraud, and such victims may be employees and customers of the financial sector of the economy. The originality of the paper lies in the fact that it uniquely combines psychological, socio-demographic and online behaviours to develop a comprehensive theoretical framework and predict susceptibility to cyber fraud. It is important that this paper describes methods of protecting users of government websites from fraud.

The opinion of Petratos (2021) is interesting, as he emphasises that information is a new cyber risk because it includes disinformation and fake news. The article suggests ways to overcome misleading information and cyber risks for business executives and leaders in various sectors of the economy.

DOI: 10.55643/fcaptp.3.62.2025.4702

Bozkus and Caliyurt (2018) analyse approaches to cybersecurity to identify key issues and weaknesses from an internal audit and risk management perspective. The digitalisation of business is gaining popularity, and digital data-creating IT ecosystems is a potential area of interest for attackers. The authors are convinced that cyber risks cannot be avoided, but they need to be managed through cyber control.

The purpose of Aleem and Ryan (2012) is to critically examine the vulnerability of a cloud platform that affects business processes. The interviewed respondents recognised data loss and leakage as the main threat to cloud computing. The authors do not focus on this, but we believe that it is important when storing financial documents in the cloud space, as there are significant risks of unauthorised access to them.

Shackelford (2012) points out that businesses are increasingly turning to cyber risk insurance to better manage cyber threats and any legal liability associated with data breaches. The author argues that it is necessary to take a proactive approach to managing cyber attacks.

Mahmud and Haq (2021) conducted a bibliometric review of the 100 most cited articles from the Web of Science database on information security in a business context. It was found that the most frequently cited articles were published between 1990-2018 and received 3375 citations. Cybersecurity policy is recognised as the most researched topic, with the majority of articles published in quartile (Q1) journals. This study identifies trends and patterns in research publications on information security in the business and financial sectors of the economy. In turn, Bolbot et al. (2022) conducted a systematic literature review and bibliometric analysis of the development of research in the field of maritime cybersecurity. This indicates the relevance of conducting bibliometric research in various areas of economic activity. The literature review identified studies that conducted bibliometric analysis with regard to cyber risks (Radanliev and De, 2021; Altarturi et al., 2020) but none related to the financial sector. Thus, a bibliometric review of cyber risks in the financial sector should focus on finding synergies between IT innovations, entrepreneurship, and financial mechanisms to overcome the risks that may result from cybersecurity breaches.

AIMS AND OBJECTIVES

The purpose of this paper is to search for and identify cyber risks in the financial sector, formulate their classification and monitor them through a bibliometric study of scientific papers in the Scopus database.

To achieve this goal, the following tasks have been formulated:

- to identify and characterise possible cyber threats and cyber risks in the financial sector;
- to conduct a bibliometric analysis of scientific papers using the keyword 'cyber AND risk';
- to form a matrix of the relationship between bibliometric clusters and possible cyber risks in the financial sector.

METHODS

The presented paper uses a combination of methods and approaches, which allows to implement the conceptual unity of the study. The systemic method was used to identify the key cyber threats to the financial sector that create cyber risks; the structural method allowed to formulate cyber risks in the financial sector of the economy. The application of the comparative method made it possible to identify the advantages and disadvantages in scientific papers on cyber risk trends. The method of analysis and synthesis using a bibliometric review allowed to identify scientific clusters and keywords that are actively involved in the study of cyber risks; the graphical method was used to summarise bibliometric data in the form of visualisation maps.

To conduct the bibliometric study, a keyword search was conducted in the Scopus scientometric database. The data were processed using the VOSviwer software (version 1.6.20) and visualisation maps of the relationship between scientific interests in cyber risks were constructed. The method of scientific abstraction was used to substantiate the relationship between the scientific cluster and cyber risk in order to determine the priority areas for eliminating cyber risks in the financial system.

RESULTS

The financial sector in the economy involves the operation of financial institutions that store collected information from a certain number of customers. That is why the banking sector is one of the most susceptible to cyber threats. In order to

increase customer satisfaction, financial institutions need to be able to withstand cyber attacks and take confident steps to minimise their consequences, namely cyber risks.

The implementation of innovative ways to counter existing threats has forced fraudsters to use new tricks, and therefore, risk mitigation methods should be adapted to the current environment. In order to prevent significant financial losses and a decrease in reputational capital, financial institutions should take a number of measures to ensure system security in general and to avoid cyber threats in particular. Such measures may include: assessing current security measures, delegating cybersecurity services to an external trusted stakeholder, and using multi-factor authentication. In this way, even if attackers steal customer registration data, the system will have an additional level of protection that will make it impossible to gain access to customer data.

In addition, cyber insurance is becoming particularly relevant as it helps to contain legal costs, inform customers about breaches, and cover the costs of repairing damaged systems and restoring electronic databases (Shackelford, 2012; Mukhopadhyay et al., 2013; (Eling and Schnell, 2016). Training and professional development of staff, studying digital descriptors is already a common practice that helps to avoid risks (Shestack et al., 2023; Ziniuk et al., 2022). We should not forget about informing customers about the methods of stealing their personal information and funds used by cybercriminals. Such methods are the most common and allow financial institutions to more easily counter cyber threats.

In the financial sector, the most serious cybersecurity threats include phishing, spoofing, malware attacks, remote work, cloud attacks, the Internet of Things, unencrypted data, and smartphone viruses. Let's take a closer look at the specifics of each.

1. Cyber risks associated with remote work. In the context of the COVID-19 pandemic and martial law, remote work has become a common practice in various areas of business, including the financial sector. Remote employees do not always work directly from home, as cafes, coworking spaces or resilience centres have become commonplace for workplace arrangements. Such work exposes them to additional risks that may arise from data breaches. Usually, banking IT specialists are unable to ensure full software security and an appropriate control system. Thus, remote work carries more potential cybersecurity threats. Therefore, financial systems should ensure that employees are aware of potential threats. It is important to recognise them in a timely manner in order to stay safe in a remote working environment and to be able to protect your electronic services.

2. Artificial intelligence. technologies in the financial sector are mainly used to create financial applications. However, AI-based tools can also be used by cybercriminals to develop intelligent malware and deliver malicious code bypassing innovative security systems.

3. Phishing. Customers of financial systems may receive threatening emails disguised as official communications. Attackers may also demand personal data from customers to use it for fraudulent purposes. In this way, they can gain access to financial information and steal funds from accounts. Similar attacks are also aimed at employees as cybercriminals gain access to credentials.

4. Unencrypted data. Data stored on a banking device that remains unencrypted poses many potential threats to customers and employees. In general, we get open access to information that can be used against the institution, its employees or customers.

5. Internet of Things (IoT). New cyber threats are a stable trend today, especially with the development of 5G networks. Since the 5G network is relatively new, its communication architecture has many bottlenecks that have not yet been fully explored, which increases the vulnerability of systems to external threats and the possibility of data leakage.

6. Viruses and malware for smartphones. With the growing popularity of mobile banking, gadgets are at constant risk. As customers switch to cashless payments and store sensitive data on their mobile devices, smartphones are becoming a target for hackers (Bongomin and Ntayi, 2020).

7. Fraud and identity theft. These cyberattacks are not new to the financial sector, but they are still quite successful for attackers. Fraudsters are often interested in customers applying for services such as payday loans, taking advantage of quick processing and sensitive financial information.

8. Malicious software. Every year, such software becomes more sophisticated and causes many problems for the banking sector and financial institutions involved in payment processing. Cybercriminals infect computers with malware, usually through phishing emails, and flash drives, and restrict access to some data through encryption. Malware attacks can lead to serious consequences, such as disruption of the company's information system, financial losses and reputational damage.

DOI: 10.55643/fcaptp.3.62.2025.4702

9. Cyber attacks using cloud technologies. Attacks on the cloud are becoming popular because financial services mostly store information in the cloud.

10. Spoofing. A common practice is to create a fake domain, which is a threat to inattentive customers. Sending messages and fabricated phone calls are common methods of spoofing in the financial sector.

Certain cyber threats are increasingly affecting the financial system of centralised and decentralised finance, as well as the communications infrastructure. Each of the cyber incidents has its own IT features and allows us to summarise cyber risks, such as:

- loss of customer personal data;
- leakage of confidential information;
- financial losses;
- unauthorised access to corporate information;
- virus infection of the financial system;
- forced interruptions in system operation;
- loss of reputation or trust in electronic services.

Taking into account the above information, cyber threats and cyber risks in the financial sector are managed to achieve strategic goals that are focused on obtaining an appropriate and effective result (Figure 1).

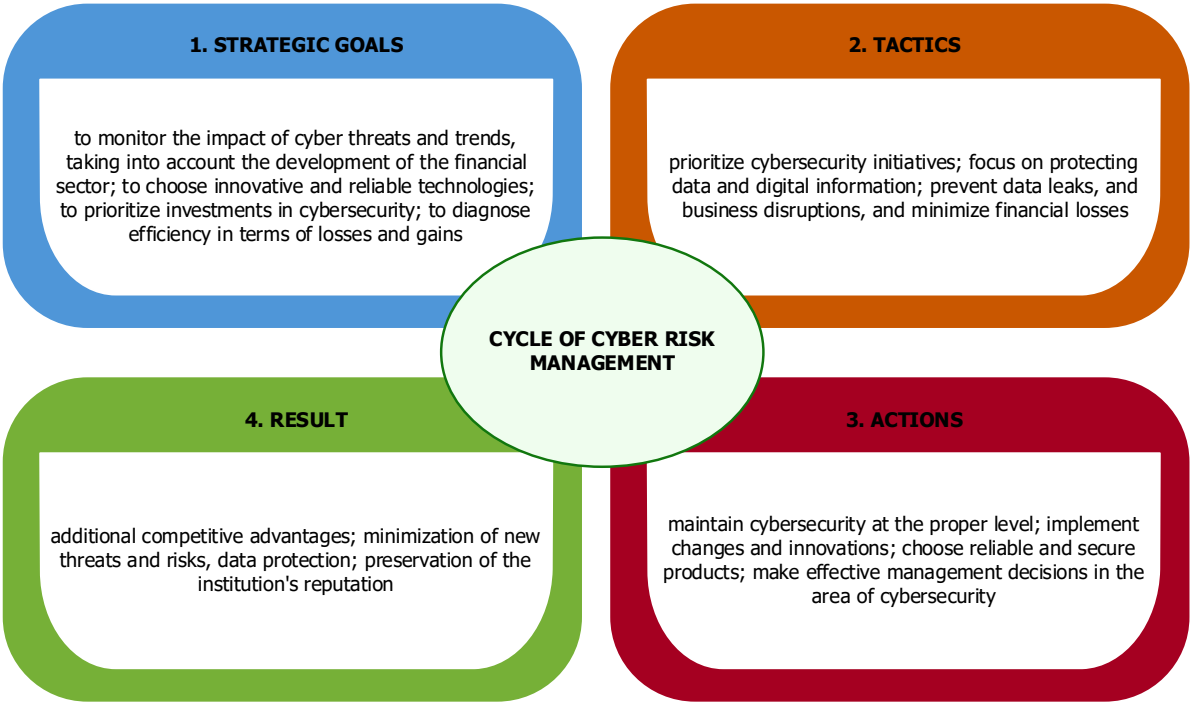

Figure 1. Cycle of cyber risk management in the financial sector of the economy.

In order to stay in the cybersecurity space, representatives of the financial sector need to pay attention to the key elements of financial cybersecurity and implement them in the operational process. This will allow to realize the defined strategic goals, choose effective tactics, and ultimately obtain reasonable results that are focused on the economic efficiency of the financial sector enterprises. Such a cycle of cyber risk management, cybersecurity issues in the financial sector, and opportunities to overcome cyber threats are increasingly becoming the subject of research by scholars and practitioners. Research results are reflected in conference abstracts, articles, books, and reviews, and are accumulated on information database sites. To substantiate the scientific opinion on the issue of cyber risks in the financial sector of the economy, documents from the Scopus scientometric database were selected.

For example, the Scopus database, which was used as the basis for the information and search research, contains a sufficient number of papers on cyber risks. By entering the keyword "cyber AND risk" in the search, we found (n=17018) papers. Cyber risk is a subject area of research in the following fields: Computer Science (n=11099), Engineering

(n=17018), Social Sciences (n=2953), Mathematics (n=2760), Decision Sciences (n=2261), Energy (n=1389), Business, Management and Accounting (n=1329), Medicine (n=1052), Physics and Astronomy (n=912), Economics, Econometrics and Finance (n=667), Psychology (n=596), Environmental Science (n=595), Materials Science (n=592), Chemical Engineering (n=292), Arts and Humanities (n=278), Earth and Planetary Sciences (n=266), Biochemistry, Genetics and Molecular Biology (n=228), Chemistry (n=172), Agricultural and Biological Sciences (n=96), Multidisciplinary (n=88) and other (n=222). The papers are categorized by country, affiliation, type of document, and language. A framework analysis of the selected papers shows that the number is growing exponentially, especially in the period from 2017 to 2024 (Figure 2). For a more accurate result, the figure does not take into account papers from 2025 (n=161).

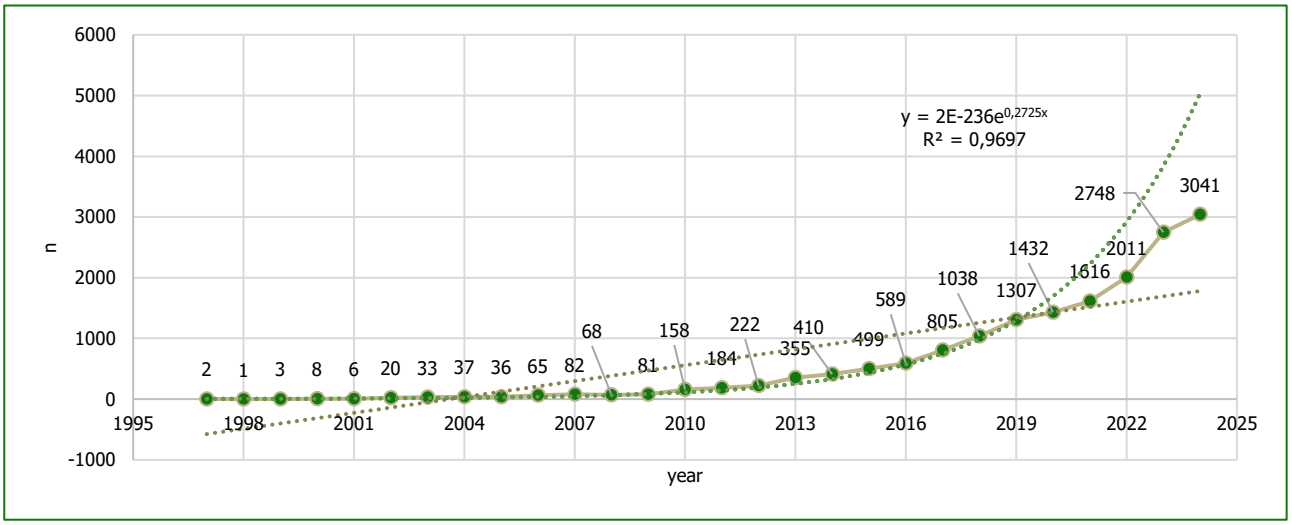

Figure 2. The dynamics of the number of scientific papers on the keyword "cyber AND risk" for 1997-2024. *(Source: presented in the Scopus database)*

According to the data presented, it was found that Nordwall (1997) first mentioned cyber threats that pose risks to the communication infrastructure, and Boyce (1997) describes cyber extortion as an element of corporate responsibility. The development of digitalization and digital technologies, the transition to Industry 4.0, and the formation of innovative technologies have contributed to the growth of scientific publications on cyber risks. Taking into account the aspects of the defined topic, namely cyber risks in the financial sector of the economy, for a more accurate bibliometric analysis, the selection of works in two subject areas was established, namely: Business, Management and Accounting; Economics, Econometrics and Finance for the period of 1999-2024. Thus, 1524 papers were selected for further review and analysis. Using the technical capabilities of Scopus, the selected papers were exported to CSV format. This formatting using the VOSviewer software allows us to see the inter-cluster relationships by keyword. In this study, at the initial stage, 3901 keywords were identified with a frequency of use of more than five times. The identified keywords are displayed in clusters on the interconnection map, based on the number of documents in which the keyword appears and its overall strength of connections with other words. The most frequently used keywords are: cybersecurity, cyber risk, risk management, information security, security, machine learning, risk, as evidenced by the data (Table 1).

Table 1. The most common keywords and the strength of their relationship on the topic of cyber risks in the financial sector of the economy. *(Source: based on data processing in VOSviewer software)*

Rank	Keywords	Occurrences	Total link strength
1	Cybersecurity	261	447
2	Cyber security	118	212
3	Cyber risk	123	207
4	Risk management	87	207
5	Information security	55	103
6	Security	50	93
7	Machine learning	39	83
8	Risk	39	81
9	Blockchain	32	69
10	Risk assessment	38	63

DOI: 10.55643/fcaptp.3.62.2025.4702

The ranking and selection of keywords were further transformed into a visualization map that represents 10 clusters and a number of relationships between them (Figure 3). The figure shows that the two largest clusters are the keywords "cybersecurity" (yellow) and "cyber risk" (red). Each of the clusters is filled with keywords related to information technology and risks in the financial sector. There is inter-citation between the clusters, taking into account the specifics of each of them. For example, the green cluster focuses on security in the information space in general, while the brown cluster focuses on management risks.

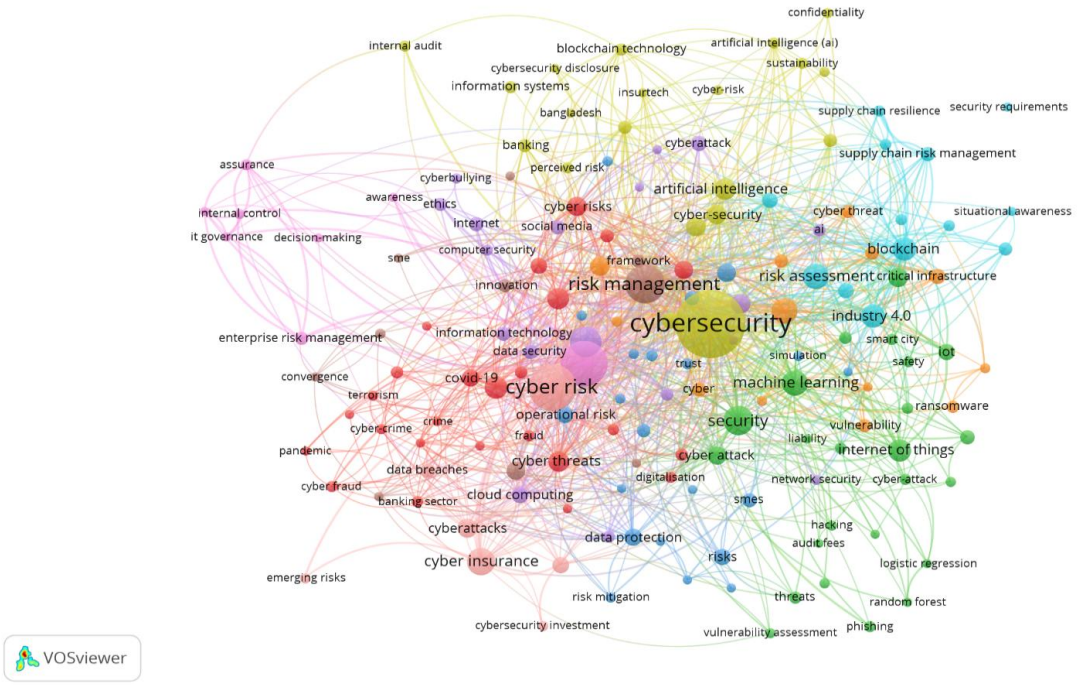

Figure 3. Keyword visualization map by formed clusters. *(Source: based on data processing in VOSviewer software)*

The analysis of scientific papers divided into clusters allows us to conclude that they are of common scientific interest. Cyber risk management helps both businesses and financial sector institutions to set goals for their corporate cybersecurity program and evaluate their progress. The authors focus on the fact that it is better to identify and prioritize cyber risks (Phair, 2024; Akyildirim et al., 2024), detect and process incidents faster (Grimwade, 2023; Biletskyi et al., 2024), and protect critical information more reliably (Biener et al., 2014; Andrew and Baker, 2021; Chiaradonna, et al., 2024). In addition, emphasis is placed on the need to improve internal and external interaction and cooperation (Li et al., 2017; Srinidhi et al., 2015; Sawik, 2013), as well as a better understanding of the shortcomings and ways to address them (Biliavskyi et al., 2024; Rahman et al., 2024).

Thus, we can observe a combination between the red cluster with the keywords "cyber risk" and the blue cluster with the keywords: business continuity, cybersecurity risk, financial stability, information sharing, operational risk, risk analysis, risks, systemic risk. The keywords and works of the blue cluster are related to the green cluster, where the keywords are: audit fees, cyber-attack, hacking, IoT, phishing, security, smart city. The visualization map shows that the yellow cluster also has a high priority, as it focuses on cybersecurity in general. This diagnosis allows us to identify three lines of defence in managing IT risks in the financial sector: audit as independent supervision and control (Lois et al., 2020; Ahmed et al., 2024; Căciulescu et al., 2024); risk management, such as determining methodology and rules, testing and monitoring (Udofia, 2024; Byatarayanapura Venkataswamy et al., 2024; Ng and Kwok, 2017) and core activities, such as implementing, executing and monitoring various types of control (Osiyevskyy et al., 2023; Aldasoro et al., 2020; Harris and Nguyen, 2024). In addition, it should be taken into account that cyber risks do not exist exclusively in the financial sector of the economy, as they are associated with certain financial transactions in manufacturing (Colabianchi et al., 2023; Strange et al., 2017), human resources management (Özgün Atalay et al., 2023; Shestack et al., 2023), procurement and logistics (Ivanov et al., 2019; Colicchia et al., 2019).

Given that the distribution by clusters (Figure 1) is a significant scientific area of research in the field of business, management and finance, it is advisable to study the dynamics of the doctype presented in the Scopus database with the highest level of citations (Table 2).

Table 2. The most cited papers on the keyword "cyber AND risk" in the financial sector of the economy. *(Source: compiled by the authors on the basis of bibliometric analysis of Scopus)*

Rank	Author, year of publication	Publications	Title	Number of citations in the Scopus database
1	Ivanov et al. (2018)	International journal of production research	The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics	1170
2	Rajapathirana and Hui (2017)	Journal of Innovation & Knowledge	Relationship between innovation capability, innovation type, and firm performance	596
3	Strange and Zucchella (2017)	Multinational Business Review	Industry 4.0, global value chains and international business	419
4	Bai (2011)	Decision Support Systems	Predicting consumer sentiments from online text	207
5	Biener et al. (2014)	The Geneva Papers on Risk and Insurance - Issues and Practice	Insurability of cyber risk: An empirical analysis	202
6	Stewart and Jürjens (2018)	Information and Computer Security	Data security and consumer trust in FinTech innovation in Germany	171
7	Ivanov et al. (2019)	Handbook of ripple effects in the supply chain	Digital supply chain twins: Managing the ripple effect, resilience, and disruption risks by data-driven optimization, simulation, and visibility	162
8	Jerman-Blažič (2008)	International Journal of Information Management	An economic modelling approach to information security risk management	158
9	Kamiya et al. (2020)	Journal of Financial Economics	Risk management, firm reputation, and the impact of successful cyberattacks on target firms	154
10	Parn and Edwards (2019)	Engineering, Construction and Architectural Management	Cyber threats confronting the digital built environment: Common data environment vulnerabilities and blockchain deterrence	143

From the above table, it can be concluded that works in various areas are of significant scientific interest. Jerman-Blažič (2008) presents an economic modelling approach to information security risk management (Rank 8), as well as the possibility of risk-based business insurance. Kamiya et al. (2020) also consider risk management, corporate reputation and the impact of successful cyberattacks on specific organisations (Rank 9) and as a result propose a model according to which an enterprise has an optimal impact on cyber risk. In turn, Stewart and Jürjens (2018) focused on the study of data security and consumer confidence in FinTech innovations (Rank 6) in Germany. This fact confirms that cyber risks in the financial sector of the economy are of interest to representatives of various countries (Hurani et al., 2024; Hanif and Lallie, 2021), as well as distinctive features in trends depending on the region or economic development.

Further study of the bibliometric data allowed us to build a network map of interrelationships by country (Figure 4) to build a network map of relationships between scientists by country.

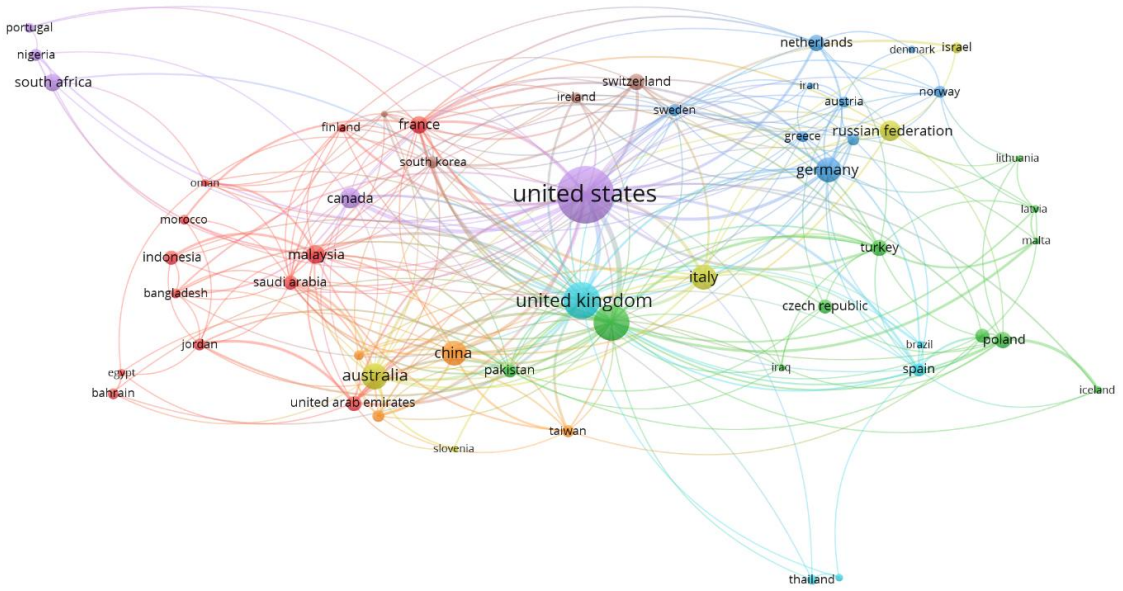

Figure 4. Network map of connections between the works of scientists in the field of cyber risks in the financial sector in different countries of the word. *(Source: Based on data processing in VOSviewer software)*

DOI: 10.55643/fcaptp.3.62.2025.4702

The study found that most studies were published in the United States (24.74%) and the United Kingdom (9.93%), which is associated with the progressive development of these countries in the field of information technology, the development of Industry 4.0, and economic and financial stability. The VOSviewer software has determined the ranking of countries by the number of documents, citations, and strength of links according to the established criteria (Table 3).

Table 3. The density of the relationship between citations by country. *(Source: based on data processing in VOSviewer software)*

Rank	Country	Documents	Citations	Total link strength
1	United States	377	4963	151
2	United Kingdom	152	2354	95
3	India	149	875	79
4	Australia	76	991	37
5	Germany	73	2154	37
6	Italy	70	1297	38
7	China	70	1213	36
8	Russian Federation	51	1534	15
9	Canada	47	390	29
10	Malaysia	40	339	42

The study of the TOP-10 mutual citations between representatives of different countries shows a description of general trends in risks and cybersecurity issues in the financial sector of the economy. The common interest in cyber risks encourages authors to find synergistic solutions in studying the evolution of the trend in which countries develop or adopt cybersecurity frameworks for use at the national level. For example, Dedeke and Masterson (2019) compare the cybersecurity frameworks developed in three countries, namely: Australia, the United Kingdom, and the United States. A related paper is the review by Hashem (2019), which focuses on the background and search for key efforts to create and implement a national cybersecurity strategy for Egypt. With the progress in modernization, there has been a penetration of information and communication technologies around the world, including Nigeria (Osho and Onoja, 2015), and in some countries, the key focus is on assessing the implementation and development of cybersecurity policies and their impact on the global cybersecurity index, such as in Georgia (Napetvaridze and Chochia, 2019). Thus, we can trace not only the mutual citations between scholars by country but also the peculiarities of cyber risk management in different countries.

The diagnostics carried out by means of a bibliometric review of the presented scientific papers in the Scopus database allows us to assess the relationship between the formed scientific clusters and the identified cyber risks (Table 4). This relationship demonstrates the influence of keywords on risk formation. For the matrix, we selected keywords for the 10 identified clusters and the identified cyber risks in the financial sector. The relationship between the words and risks was assessed on a point scale, namely: 1 point - weak correlation (green squares); 2 points - moderate correlation (yellow squares); and 3 points - strong correlation (blue squares). This made it possible to determine the overall risk level for each of the clusters, ranging from 7 to 21 points.

Table 4. Matrix of the relationship between the bibliometric cluster and possible cyber risks in the financial sector of the economy.

Clusters	Keyword	Cyber risks in the financial sector of the economy							Risk level, point
		Loss of customer personal data	Leakage of confidential information	Financial losses	Unauthorized access to corporate information	Infection of the financial system with a virus	Forced interruptions in the system's operation	Loss of reputation or trust in electronic services	
Cluster 1 Red (25 items)	banking sector, banks, COVID-19, cyber fraud, cyber resilience, cyber risks, cyber threats, cyber-attacks, cybercrime, cybersecurity awareness, digital economy, fintech, money laundering	3	1	2	1	2	3	3	15
Cluster 2 Green (24 items)	audit fees, cyber-attack, hacking, IoT, phishing, security, smart city	1	2	3	2	3	3	2	16
Cluster 3 Blue (21 items)	business continuity, cybersecurity risk, financial stability, information sharing, operational risk, risk analysis, risks, systemic risk	1	2	2	1	2	3	1	12
Cluster 4 Yellow (20 items)	banking, blockchain technology, confidentiality, cyber-risk, cybersecurity, information systems, law, regulation, sustainability	1	2	3	1	2	2	1	12
Cluster 5 Purple (18 items)	cloud computing, computer security, cyber-crime, cyberattack, cyberbullying, cyberthreats, data security, information security, information technology, reputation, social media	2	3	2	2	2	1	3	15
Cluster 6 Blue (13 items)	big data analytics, cyber-physical system, digital twin, industry 4.0, risk assessment, security requirements, supply chain risk management	1	3	2	1	2	1	1	11
Cluster 7 Orange (13 items)	attack, critical infrastructure, cryptocurrency, cyber, cyber-attacks, cyber threat, management, risk	3	3	3	2	3	3	3	20
Cluster 8 Brown (10 items)	digital technologies, innovation, it security, risk management	1	1	1	1	1	1	2	8
Cluster 9 Lilac (8 items)	auditing, cyber security, internal control, it governance	1	1	1	1	1	1	1	7
Cluster 10 Pink (7 items)	cyber insurance, cyber risk, cyberattacks, cybersecurity investment, data breaches, emerging risks	3	3	3	3	3	3	3	21

The summarized data in the table show that the lowest degree of risk in the financial sector of the economy is revealed by scientific papers that fall into clusters 8 and 9 by keywords. This is due to the narrow specialization of cyber risk research, such as focusing on cyber insurance and auditing (Lois et al., 2020; Ahmed et al., 2024; Căciulescu et al., 2024) or technological innovations and their ability to create cyber risks (Colabianchi et al., 2023; Rahman et al., 2024). However, such works are relevant because the visualization map shows a fairly high level of importance of keyword circles in these clusters. In this study, the six clusters received a somewhat similar degree of risk, ranging from 11-16 points. This indicates that the keywords in the clusters are similar to those in the research papers that focus on cyber risks in the financial sector but under different conditions. One of the most common risks is the loss of customer data, but the reasons for this can be radically different, ranging from the impact of COVID-19 and the total transition to online services to the customer's inability to follow online security rules. The leakage of confidential information has the highest power in clusters 5-6 because the keywords are focused on cyberattacks when working with data.

The next risk is financial losses, which usually arise when resources are saved that are intended to ensure the smooth operation of electronic services and protect data. This risk has the highest level of interconnectedness in clusters 2, 4, 7, and 10. Unauthorized access to corporate information and dissemination of corporate data is one of the key risks that contribute to the leakage of financial data, personnel or management documents of a financial institution. The issue of financial system virus infection has long been the focus of IT professionals and scientists, as malware that penetrates a device always aims to infect, disrupt system performance and damage data. It is capable of infiltrating the code of other software and spreading across the network. Such actions lead to information theft, data deletion, file corruption, and even cause the device to fail. The relevance of such a cyber risk is confirmed by the keywords defined in clusters 2 and 4: cyber attack, hacking, IoT, phishing, security, cloud computing, computer security, cybercrime, cyberattack, cyberbullying, cyberthreats, data security, information security, information technology.

DOI: 10.55643/fcaptp.3.62.2025.4702

The cyber threats discussed above often lead to such risks as forced interruptions in the system's operation and time spent on its recovery. Financial systems are a continuous process of work: an Internet site, banking, a digital city - so disruption of any process makes it impossible for a client to perform planned transactions. Cluster 7 contains the following keywords: attack, critical infrastructure, cryptocurrency, cyber, cyber attacks, and cyber threat, which confirm the risk of system interruptions.

A special place in the analysis of cyber risks in the financial systems sector is occupied by the loss of reputation and trust in electronic services, which is becoming increasingly important every year, but scientists and practitioners lack a consensus on finding the best solution to overcome them. Also, the study found that the highest degree of risk is revealed by scientific papers that belong to clusters 7 and 10 according to keywords. This is confirmed by the fact that these clusters contain the keywords: cyber risk, cyber attacks, cyber, cyber attacks, and cybersecurity investment.

Thus, monitoring and bibliometric review have helped to shape the key aspects of successful cyber risk management. Compliance with cybersecurity rules is key to overcoming cyber risks, as it protects customers from loss of funds and leakage of personal and corporate data. By ensuring stable and information-secure operations, financial institutions can improve their reputation, enhance customer service, and ultimately gain stable organizational and economic performance.

DISCUSSION

In this paper, a number of positions related to the formation of cyber risks in the financial sector of the economy can be considered controversial issues. Currently, scientific and practical approaches are focused on the fact that cyber risks arise due to non-compliance with cybersecurity rules. This is definitely a key information trend, but it is also appropriate to take into account other factors, such as corporate risks since the loss of trust in electronic services is a loss of reputation of a financial institution.

The key focus of the study is on the bibliometric analysis of scientific papers on cyber risks in the financial sector of the economy.

The analysis allowed us to continue the study by Nobanee (2023), which evaluated the works related to cybersecurity risks in the period 1999-2021. The study reveals various findings, including the most influential authors and leading: countries, journals, documents, financial institutions and affiliates that publish works on cybersecurity risks. We agree with the author that the bibliometric analysis shows how existing research has influenced knowledge about the consequences of cybersecurity risks. However, the paper does not focus on the key cyber risks in the financial sector of the economy, namely, it does not set limits on the subject areas related to finance and economics.

Arora and Jain (2021) discuss the various threats to cybersecurity and also highlight the various due diligence methods used to combat these threats. This opinion is important because it is the knowledge that allows avoiding cyber risks that may arise in the financial sector of the economy.

The limitation of the presented work is that the bibliometric analysis is not an accurate result of the study, despite the fact that clear time periods were selected. Search engines can display data in different ways, and therefore there is a certain error in the number of papers selected for analysis. Another limitation is that the research papers were selected from the Scopus scientometric database. This, in turn, is a disadvantage because there are a significant number of papers in sources that are indexed in: Web of Science, OpenAlex, or Crossref. However, the advantage is that there is no duplication if a scientific source is indexed in several scientometric databases.

Different from previous studies, this paper is the first to identify key cyber risks in the financial sector and to correlate them with scientific clusters formed as a result of the diagnosis of the works. Customer and employee mistakes are at the top of the list of factors that most threaten cybersecurity in the financial sector. Therefore, such institutions should warn their customers and employees about possible risks in a timely manner, and train them on how to protect confidential data and counter cyber threats. In addition, financial institutions need to be able to establish secure transactions with customers, as they are the key interests of cybercriminals. This includes not only customers but also payment processing companies. Due to their important role in processing confidential data, financial sector participants are often exposed to threats such as malware, phishing, spoofing and other cyberattacks. Payment systems are a lucrative target for cybercriminals. Therefore, to mitigate these risks, financial sector institutions should apply advanced communication infrastructure and advanced cybersecurity measures. These measures can be described scientifically and implemented in practice. First and foremost, attention should be paid to multi-level encryption and continuous monitoring of the financial system.

CONCLUSIONS

Based on the conducted research, it was found that cyber risks as an element of information security in the financial sector of the economy require a strategic vision, careful planning of tactics, and actions and regular monitoring. Internal and external cyber threats require constant and effective improvement in order to protect information systems, electronic resources and reputational capital. Given the identified cyber threats and associated risks, there is a need not only to respond to incidents but also to prevent them by systematically improving the information security of the communication infrastructure.

The paper systematizes scientific clusters using bibliometric analysis and establishes that the most used keywords in the study of cyber risks in the financial sector of the economy are: cybersecurity, cyber risk, risk management, information security, security, and risk. The search resource of the scientometric database revealed (n=1524) papers with the established limitation of areas: Business, Management and Accounting; Economics, Econometrics and Finance.

Data processing by the VOSviewer software (version 1.6.20) formed 10 scientific clusters with a clearly established relationship between scientific clusters and cyber risks in the financial sector. The constructed correlation matrix made it possible to determine the degree to which each individual cluster is associated with one of the following risks: loss of customer data; leakage of confidential information; financial losses; unauthorized access to corporate information; infection of the financial system with a virus; forced interruptions in the system; loss of reputational capital or trust in electronic services. Thus, cyber risk management in the financial sector is a certain foundation for any cybersecurity action.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & information technology*, *33*(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787
2. Ahmed, M., Alasad, Q., Yuan, J.S., & Alawad, M. (2024). Re-Evaluating Deep Learning Attacks and Defenses in Cybersecurity Systems. *Big Data and Cognitive Computing*, *8* (12), 191. https://doi.org/10.3390/bdcc8120191
3. Akyildirim, E., Conlon, T., Corbet, S., & Hou, Y.G. (2024). HACKED: Understanding the stock market response to cyberattacks. *Journal of International Financial Markets, Institutions and Money*, *97*, 102082. https://doi.org/10.1016/j.intfin.2024.102082
4. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector. *International Journal of Central Banking,* 341-402. https://www.ijcb.org/journal/ijcb23q5a8.pdf
5. Aleem, A., & Ryan Sprott, C. (2012). Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime*, *20*(1), 6-24. https://doi.org/10.1108/13590791311287337
6. Altarturi, H.H., Saadoon, M., & Anuar, N.B. (2020). Cyber parental control: A bibliometric study. *Children and Youth Services Review*, *116*, 105134. https://doi.org/10.1016/j.childyouth.2020.105134
7. Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, *168*, 565-578. https://doi.org/10.1007/s10551-019-04239-z
8. Arora, P., & Jain, A. (2021, December). Cyber security threats and their solutions through deep learning: A bibliometric analysis. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1944-1949). IEEE. https://doi.org/10.1109/ICAC3N53548.2021.9725480
9. Bai, X. (2011). Predicting consumer sentiments from online text. *Decision Support Systems*, *50*(4), 732-742. https://doi.org/10.1016/j.dss.2010.08.024
10. Biener, C., Eling, M., & Wirfs, J.H. (2014). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*, 131-158. https://doi.org/10.1057/gpp.2014.19

DOI: 10.55643/fcaptp.3.62.2025.4702

11. Biletskyi, O., Kolesnyk, T., Shymanovska-Dianych, L., Spitsyna, A., Shkoda, M., & Krasnoshtan, O. (2024). Innovative management of integrated business structures in the financial mechanism of post-war recovery. *Financial and Credit Activity: Problems of Theory and Practice, 6*(59), 293-310. https://doi.org/10.55643/fcaptp. 6.59. 2024.4663

12. Biliavskyi, V., Biliavska, Y., Umantsiv, Y., Shestack, Y., Zhurba, O., & Khavanov, A. (2024). Digital technologies in the financial sector of the economy. *Financial and credit activity problems of theory and practice*, *4*(57), 171-183. https://doi.org/10.55643/fcaptp.4.57.2024.444

13. Birindelli, G., & Iannuzzi, A.P. (2024). The Systemic Importance of Cyber Risk in Banks. In *Systemic Risk and Complex Networks in Modern Financial Systems* (pp. 301-321). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-64916-5_16

14. Bolbot, V., Kulkarni, K., Brunou, P., Banda, O.V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, *39*, 100571. https://doi.org/10.1016/j.ijcip.2022.100571

15. Bongomin, G.O.C., & Ntayi, J.M. (2020). Mobile money adoption and usage and financial inclusion: mediating effect of digital consumer protection. *Digital Policy, Regulation and Governance*, *22*(3), 157-176. https://doi.org/10.1108/DPRG-01-2019-0005

16. Boyce, B. (1997). Cyber extortion – The corporate response. *Computers & Security*, *16*(1), 25-28. https://doi.org/10.1016/S0167-4048(97)85784-7

17. Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial auditing journal*, *33*(4), 360-376. https://doi.org/10.1108/MAJ-02-2018-1804

18. Byatarayanapura Venkataswamy, S., Patil, K.S., Narayanaswamy, H.K., & Veerabadrappa, K. (2024). Access management based on deep reinforcement learning for effective cloud storage security. *International Journal of System Assurance Engineering and Management*, 1-20. https://doi.org/10.1007/s13198-024-02596-1

19. Căciulescu, A. R., Rughiniș, R., Țurcanu, D., & Radovici, A. (2024). Mapping Cyber-Financial Risk Profiles: Implications for European Cybersecurity and Financial Literacy. *Risks*, *12*(12), 200. https://doi.org/10.3390/risks12120200

20. Chiaradonna, S., Jevtić, P., Lanchier, N., & Pesic, S. (2024). Framework for Cyber Risk Loss Distribution of Client-Server Networks: A Bond Percolation Model and Industry Specific Case Studies. *Applied Stochastic Models in Business and Industry*, *40*(6), 1712-1733. https://doi.org/10.1002/asmb.2896

21. Colabianchi, S., Bernabei, M., Costantino, F., Romano, E., & Falegnami, A. (2023). MARLIN Method: Enhancing Warehouse Resilience in Response to Disruptions. *Logistics*, *7*(4), 95. https://doi.org/10.3390/logistics7040095

22. Colicchia, C., Creazza, A., & Menachof, D.A. (2018). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), 215-240. https://doi.org/10.1108/SCM-09-2017-0289

23. Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(1), 698. https://doi.org/10.1057/s41288-022-00266-6

24. Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information & Computer Security*, *27* (3), 373-392. https://doi.org/10.1108/ICS-10-2018-0122

25. Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17* (5), 474-491. https://doi.org/10.1108/JRF-09-2016-0122

26. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(6), 93-125. https://doi.org/10.1111/rmir.12169

27. Grimwade, M. (2023). The potential impacts of the digital revolution on the operational risk profiles of banks. *Journal of Risk Management in Financial Institutions*, *17*(1), 71-88. https://doi.org/10.69554/FFSP1788

28. Hanif, Y., & Lallie, H.S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. *Technology in Society*, *67*(2), 101693. https://doi.org/10.1016/j.techsoc.2021.101693

29. Harris, O., & Nguyen, T. (2024). Asset redeployability and the market reaction to cyberattacks. *Finance Research Letters*, *70*(2), 106278. https://doi.org/10.1016/j.frl.2024.106278

30. Hashem, S. (2019). Towards a National Cybersecurity Strategy: The Egyptian Case. *Journal of Systemics, Cybernetics and Informatics*, *17*(3), 88-94. https://www.iiisci.org/journal/pdv/sci/pdfs/SA867CS19.pdf

31. Hurani, J., Abdel-Haq, M.K., & Camdzic, E. (2024). FinTech Implementation Challenges in the Palestinian Banking Sector. *International Journal of Financial Studies*, *12* (4), 122. https://doi.org/10.20944/preprints202411.0832.v1

32. Ivanov, D., Dolgui, A., & Sokolov, B. (2018). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International journal of production research*, *57*(3), 829-846. https://doi.org/10.1080/00207543.2018.1488086

33. Ivanov, D., Dolgui, A., Das, A., & Sokolov, B. (2019). Digital supply chain twins: Managing the ripple effect, resilience, and disruption risks by data-driven optimization, simulation, and visibility. *Handbook of ripple effects in the supply chain*, 309-332. https://doi.org/10.1007/978-3-030-14302-2_15

34. Jerman-Blažič, B., & Borka, J. (2008). An economic modelling approach to information security risk management. *International Journal of Information*

Management, 28(5), 413-422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

35. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R.M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019
36. Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80. https://doi.org/10.1016/j.ijcip.2015.02.002
37. Li, H., Luo, X. R., Zhang, J., & Sarathy, R. (2017). Self-control, organizational context, and rational choice in Internet abuses at work. *Information & Management*, *55*(3), 358-367. https://doi.org/10.1016/j.im.2017.09.002
38. Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Business*, *15*(2), 205-217. https://doi.org/10.1108/EMJB-07-2019-0097
39. Mahmud, M., Haq, I. U. et al. (2021). Information security in business: a bibliometric analysis of the 100 top cited articles. *Library Philosophy and Practice*, 1-49. https://digitalcommons.unl.edu/libphilprac/5354/
40. Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims. *Children and Youth Services Review*, *34*(1), 63-70. https://doi.org/10.1016/j.childyouth.2011.08.032
41. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S.K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems, 56*(1), 11-26. https://doi.org/10.1016/j.dss.2013.04.004
42. Napetvaridze, V., & Chochia, A. (2019). Cybersecurity in the Making–Policy and Law: a Case Study of Georgia. *International & Comparative Law Review/Mezinárodní a Srovnávací Právní Revue*, *19*(2), 155-180. https://doi.org/10.2478/iclr-2019-0019
43. Ng, A.W., & Kwok, B.K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, *25(*1), 422-434. https://doi.org/10.1108/JFRC-01-2017-0013
44. Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M., & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime*, *30*(6), 1736-1754. https://doi.org/10.1108/JFC-11-2022-0287
45. Nordwall, B.D. (1997). Cyber threats place infrastructure at risk. *Aviation Week & Space Technology*, *146* (27), 51-51.
46. Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of Nigeria: a qualitative analysis. *International Journal of Cyber Criminology*, *9*(1), 120. https://doi.org/10.5281/zenodo.22390
47. Osiyevskyy, O., Umantsiv, Y., & Biliavska, Y. (2023). Digital Ecosystem: A Mechanism of Economic Organization of Enterprises of the Future. *Rutgers Business Review, 8*(2), 175-194. https://ekmair.ukma.edu.ua/server/api/core/bitstreams/d200b6b0-97fd-4083-a75a-ea77c0d4214a/content
48. Özgün Atalay, M., Erdem Tunç, Y., & Ceren Erkengel, H. (2023). Cyber-Spirituality in the Workplace. In *Spirituality Management in the Workplace: New Strategies and Approaches* (pp. 359-382). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83753-450-020231016
49. Panetta, I.C., & Leo, S. (2024). Systemic Cyber Risk in the Financial Sector: Can Network Analysis Assist in Identifying Vulnerabilities and Improving Resilience? In *Systemic Risk and Complex Networks in Modern Financial Systems* (pp. 133-153). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-64916-5_8
50. Parn, E.A., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management*, *26*(2), 245-266. https://doi.org/10.1108/ECAM-03-2018-0101
51. Petratos, P.N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons*, *64*(4), 763-774. https://doi.org/10.1016/j.bushor.2021.07.012
52. Phair, N. (2024). Cyberwashing: The disconnect between cyber security claims and real practices. *Journal of Risk Management in Financial Institutions*, *18*(1), 76-83. https://doi.org/10.69554/CDCM7958
53. Radanliev, P., & De Roure, D. (2021). Epistemological and bibliometric analysis of ethics and shared responsibility-health policy and IoT systems. *Sustainability*, *13*(15), 8355. https://doi.org/10.3390/su13158355
54. Rahman, M.M., Pokharel, B.P., Sayeed, S.A., Bhowmik, S.K., Kshetri, N., & Eashrak, N. (2024). riskAIchain: AI-Driven IT Infrastructure-Blockchain-Backed Approach for Enhanced Risk Management. *Risks*, *12*(12), 206. https://doi.org/10.3390/risks12120206
55. Rajapathirana, R.J., & Hui, Y. (2017). Relationship between innovation capability, innovation type, and firm performance. *Journal of Innovation & Knowledge*, *3*(1), 44-55. https://doi.org/10.1016/j.jik.2017.06.002
56. Rampášek, M., Mesarčík, M., & Andraško, J. (2025). Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? *Computer Law & Security Review*, *56*, 106093. https://doi.org/10.1016/j.clsr.2024.106093
57. Rees, L.P., Deane, J.K., Rakes, T.R., & Baker, W.H. (2011). Decision support for cybersecurity risk planning. *Decision Support Systems*, *51*(3), 493-505. https://doi.org/10.1016/j.dss.2011.02.013
58. Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, *55* (1), 156-164. https://doi.org/10.1016/j.dss.2013.01.001
59. Shackelford, S.J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4), 349-356. https://doi.org/10.1016/j.bushor.2012.02.004

DOI: 10.55643/fcaptp.3.62.2025.4702

60. Shestack, Y., Biliavska, Y., Osetskyi, V., Mykytenko, N., & Umantsiv, Y. (2023). Devising a comprehensive method to manage digital competencies. *Eastern-European Journal of Enterprise Technologies, 3(13),* 86–97. https://doi.org/10.15587/1729-4061.2023.281933

61. Srinidhi, B., Yan, J., & Tayi, G.K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, *75*(6), 49-62. https://doi.org/10.1016/j.dss.2015.04.011

62. Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information & Computer Security*, *26*(1), 109-128. https://doi.org/10.1108/ICS-06-2017-0039

63. Strange, R., & Zucchella, A. (2017). Industry 4.0, global value chains and international business. *Multinational Business Review*, *25*(4), 174-184. https://doi.org/10.1108/MBR-05-2017-0028

64. Udofia, E. (2024). A human-centric approach to cyber risk mitigation. In *the Art of Cyber Defense* (pp. 241-259). CRC Press.

65. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

66. Whitty, M.T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277-292. https://doi.org/10.1108/JFC-10-2017-0095

67. Ziniuk, M., Dyeyeva, N., Bogatyrova, K., Melnychenko, S., Fayvishenko, D., & Shevchun, M. (2022). Digital Transformation of Corporate Governance. *Financial and Credit Activity Problems of Theory and Practice*, 5(46), 300–310. https://doi.org/10.55643/fcaptp.5.46.2022.3807

Білявська Ю., Білявський В., Шестак Я., Дєєва Н., Колесник М., Тривайло А.

МОНІТОРИНГ КІБЕРРИЗИКІВ У ФІНАНСОВОМУ СЕКТОРІ ЕКОНОМІКИ

Фінансовий сектор економіки є привабливим об'єктом для кібератак, оскільки виконує важливу роль посередництва в русі грошових коштів. Ця стаття присвячена моніторингові кіберризиків, які можуть упливати на функціонування електронних сервісів. Установлено, що в практичній царині кібератаки зростають за експонентою щороку, але й у науці приділяють значну увагу визначеній проблематиці, а саме – кіберризикам. У сучасному ринковому середовищі комунікаційна архітектура базується на тому, що фінансові установи є критично важливими для глобальної комерційної діяльності, а також операцій на місцевому, державному й міжнародному рівнях господарювання. Ключова мета роботи полягала у виявленні, класифікації та моніторингові кіберризиків, які спричинені й внутрішніми, і зовнішніми кіберзагрозами у фінансовому секторі.

За результатами дослідження встановлено, що кіберризики для фінансового сектора здебільшого стосуються: витоку даних клієнта або певної корпоративної інформації, фінансових втрат, вимушених перерв у роботі електронних сервісів і зрештою втрати репутаційного капіталу та взаємної довіри. Під час проведення бібліометричного аналізу виявлено наукові праці, у яких: охарактеризовано сутність, систематизовано методичний інструментарій, досліджено класифікації кіберризиків в умовах фінансової діяльності, а також визначено можливості їх подолання з метою забезпечення кіберстійкості. Запропоновано оригінальну матрицю взаємозв'язку між визначеними науковими кластерами та кіберризиками фінансової царини, що дозволить зупинитися на розвитку перспективних рішень щодо їх подолання.

Установи фінансового сектора економіки постійно потребують розробки рекомендацій щодо захисту від негативного впливу кіберризиків, оскільки досі користуються застарілими електронними системами, які не є стійкими до загроз можливих кібератак. Висновки підтверджують актуальність і важливість роботи з кіберризиками у фінансовій царині задля забезпечення стабільності роботи та підвищення довіри до електронних сервісів.

Ключові слова: ризик, управління, бібліометричний аналіз, кібербезпека, кібершахрайства, кіберзлочинці, кластери, комунікаційна інфраструктура, цифрові технології

JEL Класифікація: D83, G30, G32