ARMG Publishing "Thinking ahead" sciendo
Financial Markets, Institutions and Risks, Volume 7, Issue 1, 2023
ISSN (online) – 2521-1242 ISSN (print) – 2521-1250

Content and Meaning of Financial Cyber Security: a Bibliometric Analysis

http://doi.org/10.21272/fmir.7(1).145-153.2023

Vitaliia Koibichuk, https://orcid.org/0000-0002-3540-7922

Ph.D. (Economics), Associate Professor, Sumy State University, Ukraine

Tetiana Dotsenko, https://orcid.org/0000-0001-5713-2205

Ph.D. (Economics), Science Researcher, Technical University of Berlin, Germany

Corresponding author: *v.koibichuk@biem.sumdu.edu.ua*

Abstract. *Reliable cybersecurity has a decision value for economic and national security of every country. The financial sector is most susceptible to cyber-attacks, as it is one of the most important systems of society, containing a large amount of data and critical information. To provide reliable cybersecurity, government must participate actively in development and strengthening of policies. It includes establishment of rules and standards for business, creation of only national strategy of cybersecurity and participating in international partnership for an exchange advanced experience and resources. In addition, government must invest in cybersecurity tools, technology, and personnel to protect digital infrastructure and the data of citizens and companies. Finally, governments should prioritize cyber security education and awareness among citizens and companies to minimize the risk of digital attacks. The article provides a comprehensive bibliometric analysis of scientific publications devoted to the topic of financial cyber security using modern powerful bibliometric software (Vosviewer, Bibliometrix, SciVal) and an analysis of normative legislative documents of Ukraine and the European Union, in particular the recommendations of the European Union Agency for Cyber Security (ENISA). The bibliometric analysis made it possible to form groups of clusters characterizing the cyber lexicon, methods, and technologies for detecting cyberthreats, and to highlight the most cited publications in the world. The statistical basis for the analysis was formed by scientific publications indexed by the Elsevier reference and bibliographic corporation. The results of the conducted research are a plan of recommended actions for managers of financial institutions, banks, and enterprises regarding the effective organization of cyber security and includes such steps as: development of cyber security culture on an ongoing basis; appointment of a responsible person for the organization of cyber security; conducting cyber security audits on an ongoing basis; creating a data protection memo; provision of advanced training in the field of cyber data protection; ensuring effective interaction with a third party involved in financial relations, reflected in concluded contracts; formation of a response plan to cyber incidents; organization of secure access to automated information systems used in the institution's operations; organization of device security in case of remote use and performance of professional duties; organization of network connection security; improvement of physical security of official documents and devices; protection of backup copies and testing for the possibility of a full update based on these backup copies; synchronization with cloud technologies in compliance with the provisions of regulatory documents; protection of websites, publication and distribution of up-to-date information on new types and types of cyber threats.*

Keywords: bibliometric analysis, cyber security, data protection, financial system, regulatory and legal documentation.
JEL Classification: G14, G14, F52.

Type of manuscript: research paper.

Received: 5.02.2023 **Accepted:** 18.03.2023 **Published:** 31.03.2023

Funding: This research was funded by the grant "Data Mining for Countering Cyber Fraud and Money Laundering in the Context of Digitalization of the Financial Sector of the Ukrainian Economy" from the Ministry of Education and Science of Ukraine (No. s/r 0121U100467)

Publisher: Academic Research and Publishing UG (i. G.) (Germany)

Cite as: Koibichuk, V.& Dotsenko, T. (2023). Content and Meaning of Financial Cyber Security: a Bibliometric Analysis. *Financial Markets, Institutions and Risks*, *7*(1), 145-153. http://doi.org/10.21272/fmir.7(1).145-153.2023

Financial Markets, Institutions and Risks, Volume 7, Issue 1, 2023
ISSN (online) – 2521-1242 ISSN (print) – 2521-1250

Introduction

Financial cyber security has an enormous value in the modern world, is critically the important component of defense of both companies and individuals from financial losses. Also, financial cyber security is the important element of informative safety, that is concentrated on the protection of digital financial transactions, data and systems fetch and ill-intentioned actions. Financial institutions must ensure the security of their systems to protect customer data, prevent fraud and protect their reputation (Bozhenko, et.al, 2022). Investing in cybersecurity measures such as data encryption and authentication can help protect financial data, prevent hackers from accessing sensitive information, and reduce the risk of financial loss due to cybercrime. Therefore, financial cyber security is the use of technologies to protect networks, programs, computers, and data (Pakhnenko et.al, 2023) from cyber-attacks, to prevent cyber threats (Microsoft, 2023). This includes protecting against malicious attacks such as malware, phishing, and other forms of cybercrime. It also involves preventing unauthorized access to networks and data, as well as ensuring data integrity and confidentiality (Melnyk, et.al, 2022). Cybersecurity measures may include encryption, authentication, access control, firewalls, and other security measures.

Literature Review

The interest of the scientific community in the study of financial cyber security is steadily growing. Firstly, this is due to the growth in complexity and sophistication of the types of cyber threats, and secondly, the growth in the value of digital assets and the expansion of the field of financial services. As the value of digital assets increases, so does the motivation to focus on these assets. The financial services sector is also expanding, with more and more financial institutions offering digital services, increasing the potential for successful cyber-attacks. Third, the proliferation of digital technologies has increased the attack surface for attackers, making financial cybersecurity an increasingly important issue. Analyzing publications on the topic of "financial cyber security" from January 1998 to January 2023, indexed by the bibliographic and reference database Scopus, we see that the number of publications in the period from 1998 to 2014 did not exceed 50 per year, while, as in 2022 their number is 252 units, that is, it has increased more than 5 times, almost at an exponential rate (Figure 1). The total number of publications for the period from January 1998 to January 2023 was 1,650.

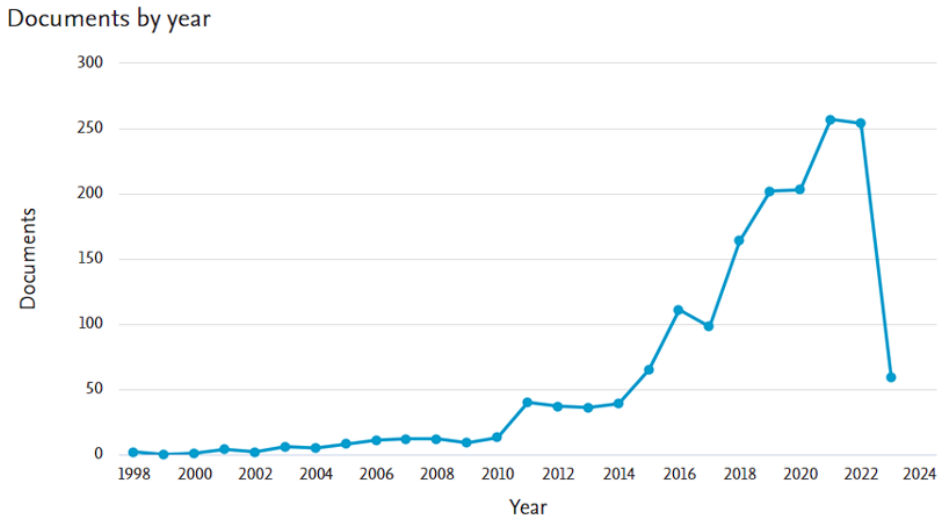

Figure. 1. Dynamics of scientific publications on the topic of "financial cyber security"

Source: compiled by the authors based on the data of the Scopus database search system

The graph of relationships of 5 or more keywords used by the authors in their research is shown in Figure 2 (see in Appendix).

The distribution of keywords is carried out in directions related to the cyber lexicon (Financial Stability Board, 2018), types of cyber threats, methods of assessing the risk of their occurrence, methods of detection and countermeasures, as well as the frequency of use in the publications found and the total number of relationships is given in Table 1.

Table 1. Distribution of keywords by the topic "financial cyber security"

Keyword	Occurrences	Total link strength
cybersecurity	243	421
cyber security	198	344
machine learning	108	237
security	103	217
blockchain	62	168
malware	38	105
internet of things	34	103
cybercrime	48	102
deep learning	42	102
phishing	41	88
information security	50	85
artificial intelligence	33	84
iot	32	82
risk management	31	72
privacy	30	71
cyber attacks	29	59
social engineering	22	59
ransomware	19	58
cyberattacks	22	54
smart grid	23	54

Source: built by the authors based on the analysis in Vosviewer software

It is also appropriate to consider the scientific fields in which researchers publish topical issues related to financial cyber security in the first city - computer science (16.2%), in the second - software engineering (13.5%), in the third - Economics, Econometrics and Finance (10.8%) and Arts and Humanities (10.8%) (Fig. 3). This analysis was carried out using the SciVal analytical system of the Elsevier publishing corporation based on the formed clusters for 2018-2022 corresponding to the topics "Cybercrime", "Computer Security".

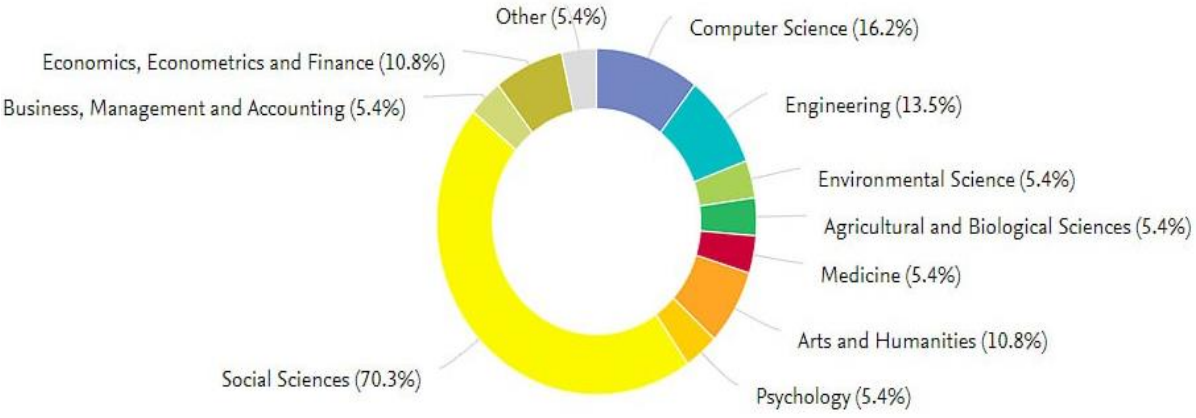

Figure 3. The share of publications on the topic "Cybercrime", "Computer Security" by subject areas

Source: built by the authors based on the analysis SciVal

From the point of view of a complex bibliometric analysis, an analysis of the citations of publications by world scientists for the last 5 years, from 2018 to January 2023, was also carried out using the Biblioshiny package and the R Studio programming language (Aria et al. 2017) (Figure 4).

Figure 4. Most Global Cited Documents

Source: built by the authors with Bibliometrx toolkits (Aria et.al, 2017)

Methodology and research methods

The methodological basis of the study was made up of the recommendations of the European Union Agency for Cyber Security (ENISA) on the effective organization of cyber security for financial institutions, small and medium-sized businesses, as well as normative and regulatory support of the Verkhovna Rada of Ukraine, the Ministry of Finance of Ukraine, and the Cabinet of Ministers of Ukraine. Bibliometric analysis programs (Vosviewer, Biblioshiny, SciVal), the Scopus database search system, and the R Studio programming language were used to determine the meaningful essence of the term "financial cyber security", keywords and subject areas.

Results

Unfortunately, with the development of digitization processes, so do cyber threats and cybercriminal schemes, especially in financial systems and the financial services industry, including but not limited to internet banking, neo banking and money transfer services, retail payment systems, mobile banking and payment systems, digital currencies, and other financial services (Lahouirich, et. al, 2021; Loucanova et. al, 2022). These threats can include theft of customer information and funds, money laundering, unauthorized transfers, and other malicious activities. In addition, cyber threats can include denial-of-service attacks, malware introduction, ransomware, phishing, social engineering, and data breaches. Attacks on financial institutions can have serious risks to the security of customers, operations, and finances. According to analyst and consulting firm Fortune Business Insights, the global cybersecurity market is projected to reach US$300.4 billion by 2025, growing at a compound annual growth rate (CAGR) of 10.6% from 2022 to 2025 (Fortune Business Insights, 2022). This growth is driven by the growing threat of cyber-attacks, increasing demand for cloud solutions, and growing demand for Internet of Things (IoT) security. In addition, growing focus on data privacy and growing need for regulatory compliance are expected to drive market growth over the forecast period. Therefore, it is extremely important for companies, banks, financial institutions, enterprises, (all socio-economic entities) to monitor the state of their cyber security and have reliable protection against potential attacks and should also apply secure customer authentication and data encryption methods to protect confidential customer data (Pillay et. al, 2022). In particular, the European Union Cyber Security Agency (ENISA) recommends following 12 steps for high-quality cyber security of small and medium-sized businesses (Table 2) (ENISA, 2021).

ISSN (online) – 2521-1242 ISSN (print) – 2521-1250

Table 2. Cyber security measures of small and medium enterprises

Event name	Brief description of the event
1. Develop a good cyber security culture: appoint a responsible person for the organization of cyber security; conduct cyber security audits; remember about data protection	1.1. Reliable cyber security is the key to sustainable development and success of any business. Therefore, it is necessary to appoint a responsible person who must provide the appropriate resources, such as staff time, acquisition of software, services and equipment for cyber security, training of staff and development of an effective cyber security policy. In addition, it is necessary to have open leadership support for cybersecurity initiatives, conduct appropriate training for employees, and provide clear, specific rules outlined in cybersecurity policies that are regularly reviewed and updated. 1.2. Policies should spell out the consequences an employee may face if the cybersecurity policy is not followed. Regular audits should be conducted by individuals who have the appropriate knowledge, skills and experience and are independent of day-to-day IT operations. 1.3. According to the EU General Data Protection Regulation, any enterprises, financial institutions that process or personal data of residents of the European Economic Area must provide appropriate security control to protect this data. This guarantees the protection of the interests of third parties working on behalf of the referring company and provides them with security measures.
2. Provide appropriate training	Conduct regular cyber security training for all employees so that they can recognize and deal with various cyber security threats. These trainings should be adapted for small businesses and focused on real situations
3. Provide effective third-party management	Ensure that all vendors, especially those with access to sensitive data and/or systems, are actively managed and meet agreed security levels. Contract agreements should specify how suppliers meet security requirements
4. Develop an incident response plan	A formal incident response plan should contain clear guidelines, roles and responsibilities documented to ensure a timely, professional, and appropriate response to all security incidents. To quickly respond to security threats, it is necessary to research and analyze tools that can monitor and generate alerts in case of suspicious activity or a security breach.
5. Secure access to systems	Use a passphrase that is a set of at least three random common words combined into a phrase that provides a very good combination of memorability and security: do not reuse elsewhere; do not share with colleagues; enable multifactor authentication; use a special password manager. If using a standard password, it is recommended to make it long, with upper- and lower-case characters and special characters. Avoid using "123", "password", personal information that is publicly available on the Internet.
6. Device security	A key step in a cybersecurity program is to secure the devices that employees use (desktops, laptops, tablets, or smartphones), so it's important to keep software patched and up to date (ideally using a centralized patch management platform). 6.1. Centrally managed antivirus software must be implemented on all types of devices and kept up to date to ensure its continued effectiveness. 6.2. Use software to block spam emails, emails with links to malicious websites, emails with malicious attachments, viruses, phishing emails. 6.3. Protection through encryption. Small and medium-sized businesses must ensure that data stored on mobile devices such as laptops and smartphones is encrypted. For data transmitted over public networks, such as hotel or airport Wi-Fi networks, ensure that the data is encrypted using a virtual private network (VPN) or accessing websites over a secure connection using SSL/TLS. Ensure that their own websites use appropriate encryption technology to protect customer data in transit over the Internet.
7. Network security	Making it easier for staff to work remotely, many SMEs allow staff to use their own laptops, tablets and/or smartphones. This raises several security concerns for sensitive business data stored on these devices. One way to manage this risk is through mobile device management. This will allow: to exercise control over the devices that are allowed to use the services and systems of SMEs; such devices must have up-to-date anti-virus software installed; access to such devices - through reliable passwords or PIN code; remotely wipe any SME data from the device if the device owner reports the device lost or stolen, or if the device owner is terminated from the SME. The next recommendation is to use firewalls and regularly check the operation and settings of devices involved in remote access to SME resources.
8. Improving physical security	Appropriate physical controls should be used wherever important information is contained. For example, a business laptop or smartphone cannot be left unattended in the back seat of a car. Every time a user leaves their computer, they must lock it. Otherwise, you must enable the auto-lock feature on any device used for business purposes. Confidential printed documents should also not be left unattended and should be stored securely when not in use.
9. Backup protection	Backups should be regular and automated, preferably encrypting backups. Conduct recovery capability testing. Ideally, full recovery testing should be done regularly from start to finish.

Table 2 (cont.). Cyber security measures of small and medium enterprises

Event name	Brief description of the event
10. Synchronize with cloud technologies	While offering many benefits, cloud solutions still present some unique risks that SMEs should consider before working with a cloud provider. ENISA has published the Cloud Security Guide for SMEs, which SMEs should refer to when moving to the cloud. When choosing a cloud provider, an SME should ensure that they are not breaking any laws or regulations by storing data, especially personal data, outside the EU/EEA. For example, the EU's General Data Protection Regulation (GDPR) requires that personal data of EU/EEA residents is not stored or transferred outside the EU/EEA, except in very specific circumstances.
11. Protection of online sites	It is imperative that SMEs ensure that their online sites are set up and maintained in a secure manner and that any personal data or financial details, such as credit card details, are properly protected. This involves conducting regular website security tests to identify any potential security weaknesses and conducting regular audits to ensure the site is properly maintained and updated.
12. Search and share information	An effective tool for combating cybercrime is the exchange of information. Sharing cybercrime information is key for SMEs to better understand the risks they face. Companies that learn about cybersecurity challenges and how those challenges have been overcome are more likely to take steps to protect their systems than if they heard similar details from industry reports or cybersecurity surveys.

Source: compiled by the authors based on ENISA (2021).

The legislative base of Ukraine, in particular the Verkhovna Rada, the Cabinet of Ministers of Ukraine, the Ministry of Finance regulates financial cyber security measures in a number of regulatory legal documents (Table 3).

Table 3. Legislative framework of financial cyber security of Ukraine

№ з/п	Name of the document	Source
1	About the main principles of ensuring cyber security of Ukraine	Law of Ukraine (No. 2163-VIII dated August 17, 2022) https://zakon.rada.gov.ua/laws/show/2163-19#Text
2	On the approval of the Regulation on the organization of cyber security of financial institutions of Ukraine	Order of the Ministry of Finance of Ukraine dated March 25, 2019 https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
3	On the approval of the List of cyber security rules of financial institutions of Ukraine	Order of the Ministry of Finance of Ukraine dated June 3, 2019 https://ips.ligazakon.net/document/JH1N268A
4	On the approval of the Rules for the protection of information against unauthorized access and use in the market of financial services	Decision of the National Commission for State Regulation in the Field of Financial Services Markets dated September 18, 2019 https://zakon.rada.gov.ua/laws/show/2664-14#Text
5	On the approval of the Regulation on the organization of cyber protection in the banking system of Ukraine and amendments to the Regulation on the identification of critical infrastructure objects in the banking system of Ukraine	Resolution of the Board of the National Bank of Ukraine dated August 12, 2022 No. 178 https://zakon.rada.gov.ua/laws/show/v0178500-22#Text
6	About financial services and state regulation of financial services markets	Document 2664-III, valid, current edition – Edition dated 07.01.2023, basis – 2154-IX https://zakon.rada.gov.ua/laws/show/2664-14#Text
7	On the approval of the Regulation on the organization of cyber protection in the banking system of Ukraine	Resolution of the Board of the National Bank of Ukraine https://bank.gov.ua/admin_uploads/article/proekt_2021-11-04.pdf?v=4
8	On the approval of the Regulation on the organizational and technical model of cyber protection	Cabinet of Ministers of Ukraine. Resolution of December 29, 2021, No. 1426 https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

Source: compiled by the authors.

Therefore, financial cyber security affects the financial stability and economic development of each country (Holobiuc, 2021) and consists in protecting financial systems from cybercrimes and other threats (Ed. Fernando Alonso Ojeda Castro, 2021). Protection of financial systems is necessary to prevent negative consequences for the economy and citizens. This allows banks, investors, and businesses to act with some confidence and assurance that their financial assets are protected. A high-quality and high level of cyber security helps protect the organization's financial information from unauthorized access, manipulation, or theft, helps ensure that all financial transactions are legal and comply with applicable laws and regulations. In addition, financial cyber security helps protect customers and stakeholders from potential financial losses and counter cyber-attacks and cyber fraud.

Conclusions

The study carried out a bibliometric analysis of the concept of "financial cyber security" using the tools Vosviewer, Biblimetrix, SciVal, which made it possible to comprehensively identify the key subject areas of scientific publications where this issue is most relevant (Computer Science, Engineering, Economics, Econometrics and Finance and Arts and Humanities), to form a database of keywords that directly define both the meaningful essence of "financial cyber security" and the methods and technologies for detecting, countering, and preventing cyber-attacks. In addition, a detailed analysis of normative legislative documents of Ukraine and the European Union, in particular the recommendations of the European Union Agency for Cyber Security (ENISA), made it possible to summarize the main steps that should be followed by managers of financial institutions for a high-quality and effective organization of cyber security: develop a culture of cyber security on an ongoing basis; appoint a responsible person for the organization of cyber security; conduct cyber security audits on an ongoing basis; create a data protection memo; provide appropriate training; to ensure effective interaction with a third party involved in financial relations, reflected in concluded contracts; have a cyber incident response plan; ensure safe access to automated systems used in the institution's operations; ensure device security in case of remote use and performance of professional duties; ensure network security; improve physical security; protect backup copies and conduct testing on the possibility of a complete update based on these backup copies; synchronize with cloud technologies; ensure website protection, publish and disseminate up-to-date information on new types and types of cyber threats.

Author Contributions

Conceptualization: Koibichuk, V.; **methodology:** Koibichuk, V.; **software:** Koibichuk, V.; **validation:** Dotsenko, T.; **formal analysis:** Koibichuk, V.; **investigation:** T.D.; **resources** Dotsenko, T.; **data curation:** Koibichuk, V.; **writing-original draft preparation:** Dotsenko, T.; **writing-review and editing:** Koibichuk, V.; **visualization:** Dotsenko, T.; **supervision:** Koibichuk, V.; **project administration:** Koibichuk, V.; **funding acquisition:** Koibichuk, V.; and Dotsenko, T.

All authors have read and approved the final manuscript.

References

1. Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959-975. [Link] [CrossRef]
2. Bozhenko, V., Mynenko, S. & Shtefan, A. (2022). Financial Fraud Detection on Social Networks Based on a Data Mining Approach. *Financial Markets, Institutions and Risks*, *6*(4), 119-124. [CrossRef]
3. Ed. Fernando Alonso Ojeda Castro. (2021). Cybersecurity, An Axis On Which Management Innovation Must Turn In The 21st Century. *SocioEconomic Challenges*, *5*(4), 98-113. [CrossRef]
4. ENISA (2021). Cloud Security Guide for SMEs. [Link]
5. ENISA (2021). Cybersecurity guide for SMEs - 12 steps to securing your business. [Link]
6. European Commission (2021). Data protection Rules for the protection of personal data inside and outside the EU. [Link]
7. Financial Stability Board (FSB): Cyber Lexicon. (2018, November, 12). [Link]
8. Fortune business insights (2022). Cyber security market. [Link]
9. Holobiuc, A.-M. (2021). Determinants of economic growth in the European Union. An empirical analysis of conditional convergence. *SocioEconomic Challenges*, *5*(2), 26-34. [CrossRef]
10. Lahouirich M. W., El Amri, A., Oulfarsi S., Sahib Eddine, A., El Bayed Sakalli H., Boutti, R. (2022). From financial performance to sustainable development: A great evolution and an endless debate. *Financial Markets, Institutions and Risks*, *6*(1), 68-79. [CrossRef]
11. Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" dated August 17, 2022 No. 2163-VIII.
12. Loucanova, E. & Olsiakova, M (2022). Comparison of Innovation in the Electronic Banking Services of the Largest Slovak Banks. *Marketing and Management of Innovations*, 4, 1-9. [CrossRef]

13. Melnyk, M., Kuchkin, M., Blyznyukov, A. (2022). Conceptualization and Measuring the Digital Economy. *Business Ethics and Leadership*, *6*(2), 127-135. [CrossRef]
14. Pakhnenko, O., & Kuan, Z. (2023). Ethics of Digital Innovation in Public Administration. *Business Ethics and Leadership*, *7*(1), 113-121. [CrossRef]
15. Pillay, H. L., Singh, J. S. K., & Fah, B. C. Y. (2022). Innovative Activity in SMEs: Critical Success Factors to Achieve Sustainable Business Growth. Marketing and Management of Innovations, 2, 31-42. [CrossRef]

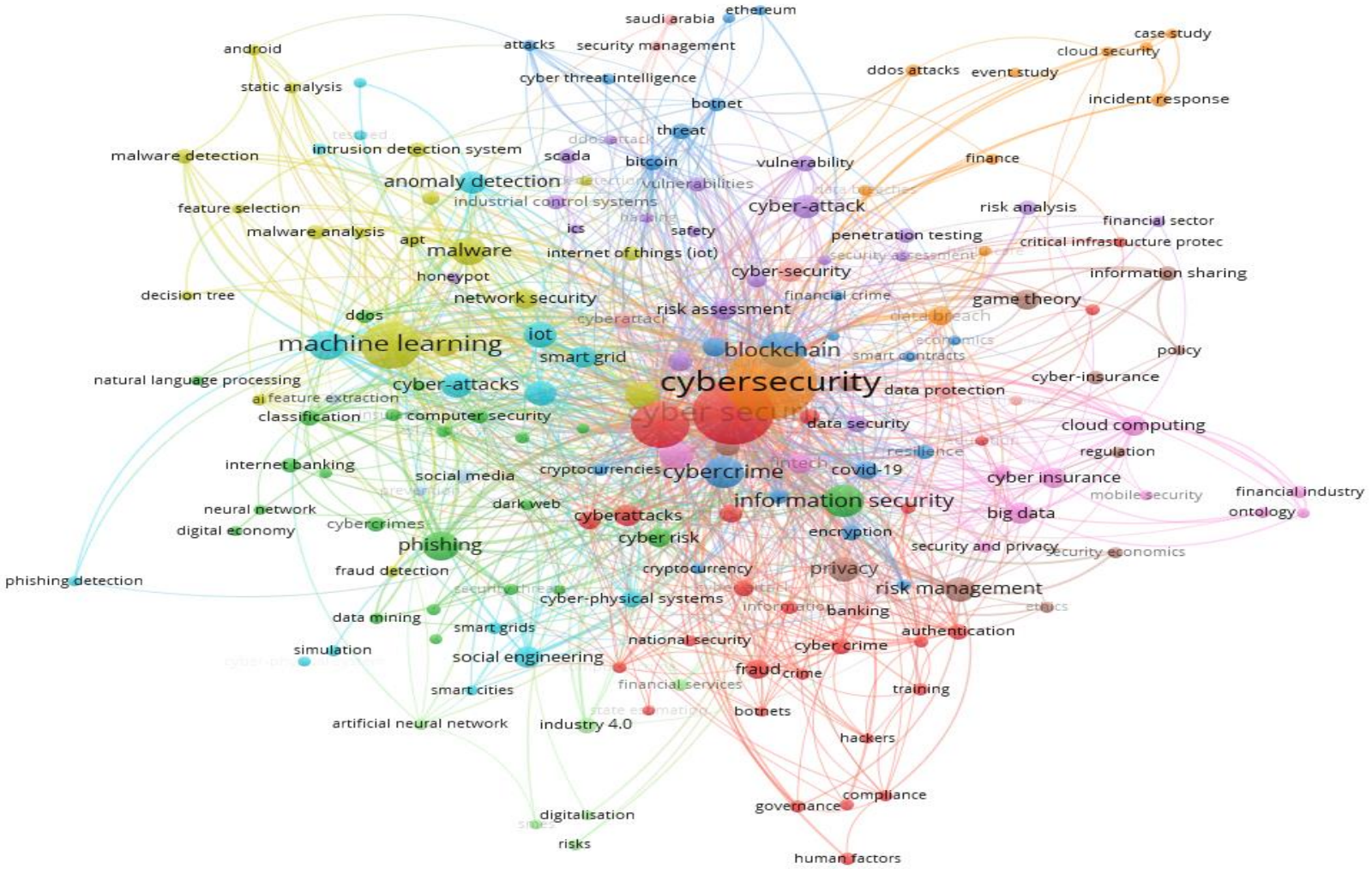

Figure 2. Map of clusters of keywords characterizing the issue of "financial cyber security"

Source: compiled by the authors with Vosviewer toolkits

Financial Markets, Institutions and Risks, Volume 7, Issue 1, 2023
ISSN (online) – 2521-1242 ISSN (print) – 2521-1250