Dynamic and bibliometric analysis of terms identifying the combating financial and cyber fraud system

http://doi.org/10.21272/fmir.6(3).93-104.2022

Hanna Yarovenko, ORCID: https://orcid.org/0000-0002-8760-6835

D.Sc., Visiting Professor of the Informatics Department, University Carlos III of Madrid, Spain; Associate Professor of the Economic Cybernetics Department, Sumy State University, Ukraine

Marina Rogkova, ORCID: https://orcid.org/0000-0002-5444-9095

PhD Student, Sumy State University, Ukraine

Abstract

The main purpose of this study is to conduct a dynamic and bibliometric analysis of the main terms that identify the system for combating financial and fraud to identify trends in the formation of social and scientific thought. The review of the scientific literature indicates an increase in the number of scientific publications over the past ten years. It was revealed that the most cited works cover the problems associated with cyber threats in everyday life, among which are botnets, cyber bullying, as well as financial fraud implemented through cryptocurrencies, smart contracts, and the black market on the Internet. Cloud forensics, technical and intellectual analysis are proposed as countermeasures. The research tools were a dynamic analysis of global network user requests, implemented using Google Trends, and a bibliometric analysis of scientific publications by the world's leading scientists, performed using the VOSviewer analytical package. The search terms "Fraud", "Finance Fraud", "Cyber Fraud", "Finance Cyber Fraud", "Money Laundering", "Anti-Money Laundering" and "Anti-Fraud" for the period from 08/07/2017 to 08/07/2022. For bibliometric analysis, two datasets with a length of 2,000 observations were formed based on queries in the Scopus database regarding the terms "Cyber Crime" and "Anti-money Laundering". The results of the dynamic analysis revealed a decrease in the level of interest in fraud and financial fraud since the beginning of 2021, while the trend of cyber fraud is increasing. This led to the conclusion that there was an impact of the pandemic, which caused an increase in cybercrime. The results of the analysis of requests for "Fraud" and "Finance Fraud" by geographical distribution showed that they interested users belonging to countries with a significant difference in economic development. That is, representatives of poor countries are potential cyber fraudsters, and developed countries are potential victims of fraud. Conducting a bibliometric analysis made it possible to obtain clusters of promising areas of scientific research in the field of cybercrimes, among which mathematical and network tools for combating them, general concepts, digitalization and digital forensics, cyber protection, data protection, authentication and encryption of data, etc. are highlighted. At the same time, the focus of research is shifting towards methods of countering cybercrimes. Promising directions in the field of Money Laundering are mathematical methods and information technologies, cryptocurrencies and blockchains, corruption, financial terrorism, etc. The greatest potential belongs to money laundering through cryptocurrencies and blockchains. The lessons learned can be useful for improving the strategy of combating financial and cybercrimes and forming an analytical basis for the scientific community and practitioners.

Keywords: Anti-Fraud, Anti-Money Laundering, Bibliometric Analysis, Cyber Fraud, Dynamic Analysis, Finance Fraud, Money Laundering.

JEL Classification: C61, G21, M15.

Received: 17.06.2022 **Accepted:** 25.08.2022 **Published:** 30.09.2022

Funding: There is no funding for this research.

Publisher: Sumy State University.

Cite as: Yarovenko, H. and Rogkova, M. (2022). Dynamic and bibliometric analysis of terms identifying the combating financial and cyber fraud system. Financial Markets, Institutions and Risks, *6*(3), 93-104. http://doi.org/10.21272/fmir.6(3).93-104.2022

Introduction

The consequences of Revolution 4.0 contributed to the active development and implementation of computer technologies in various spheres of life. In turn, such progress became the reason for the emergence of new methods and tools for committing criminal acts, taking into account the possibilities of information and cyber space. That is, a modern type of crime has appeared - cybercrime or cyberfraud, which is carried out using computer technologies and is directed against various subjects of the economy, starting from the user and ending with complex software and technical complexes of private and state institutions. According to IBM (2022), the cost of data leakage as a result of cybercrimes in 2021 was the highest in the last decade and amounted to $4.2 million. In connection with large losses from cyber threats in most developed countries of the world, the amount of expenditures aimed at ensuring cyber security has doubled in the last year alone, and among private organizations - by almost 85%, which is a record amount of expenditures for the IT sphere.

As a rule, cybercriminals try to damage software, technical, network or information support and receive a benefit in the form of a financial reward for stopping their own criminal actions, or access to the financial information of the fraud target. The last type can be identified as financial cyber fraud. Among them, the illegal execution of transactions related to the legalization and laundering of criminal proceeds, or the implementation of such operations through the Darknet, cryptocurrencies, blockchains, hacking of the banking network, computer forgery of documents, etc. are highlighted.

Most countries in the world have their own systems to combat financial and cybercrimes, but all of them have a common goal - to protect the privacy of citizens and prevent financial losses of economic entities. The organization of such systems should be based on international regulatory and legal documents regulating cyber security issues, aimed at creating a safe information space and ensuring an appropriate level of financial and economic security. One of the main such documents is the Council of Europe Convention on Cybercrime, which outlines the basic rules of international information exchange and the principles of cooperation between countries in the information space (OAS, 1994). Regarding the fight against money laundering and the financing of terrorism, The Financial Action Task Force has developed relevant recommendations that define the structure of measures for the formation of a system of combating financial crimes (FATF, 2001).

Since financial and cyber fraud can be carried out using the same methods, or one type is used to implement another, the modern system for countering such crimes should be built taking into account this aspect. Therefore, today the priority in the development of the country's information and communication sector should be the creation of a powerful and effective system for combating financial and cyber fraud, taking into account world experience.

1. Literature Review

The topic dedicated to the study of financial and cyber fraud has been relevant in academic circles in the last decade. This trend is a consequence of the Fourth Industrial Revolution, which not only contributed to the rapid development and implementation of information and communication technologies in all spheres of society's life, but also influenced the emergence of new scientific directions and schools in the field of cyber security. Cyber-fraud research began in the 90s of the 20th century. The first three scientific works, which were published in publications indexed in the Scopus database, date back to 1998. Bequai (1998) studied the problems of cyber-crime investigations, offered a Guide to cyber-crime investigations, where he considered such important concepts as data privacy and computer privacy. Benjamin et al. (1998) raised questions about the protection of information systems in various companies depending on the nature of potential cyber-attacks. Mumford (1998) revealed directions for solving the problem associated with cybercrime combined with the drug business. Since 1998 and up to our time, 2,133 scientific works have been published in publications indexed in the Scopus database.

Works that are recognized in scientific circles and have the highest citation rate deserve attention. Among them is the article by Choo (2011), in which the author investigated the risks of cyber threats in everyday activities, and also proposed potential ways to reduce them. Feily et al. (2009, June) conducted a survey that was devoted to one of the most popular cyber threats in the world - the botnet, which allowed to explain its phenomenon and classify its detection methods. Tounsi and Rais (2018) focused on technical threat analysis in their article, where they proposed appropriate strategies for its implementation and also analyzed the software market for the availability of appropriate analysis tools. Ruan et al. (2013) presented the results of a survey conducted among digital experts regarding cloud forensics, its features, problems, implementation opportunities, etc. Kolodenker et al. (2017, April) developed the PayBreak anti-ransomware system that collects files of cybercrime victims and helps decrypt and recover files without paying a ransom to the criminals. Huang et al. (2014, November) consider other aspects of the impact of cyber threats, such as social. They investigate the problems of cyber-bullying that arise in social networks and lead to negative social and psychological consequences, especially in children and adolescents.

As for financial fraud, the most popular are crimes related to the laundering of criminal proceeds and the financing of terrorism. This type is especially relevant in cyberspace, as banking transactions through mobile and Internet applications are the most common. Accordingly, many schemes are created for their implementation, which contributes to the growth of the process of legalization of criminal funds in the country. This topic has become interesting since 1990, as evidenced by the first articles published in publications that are indexed in international databases. Here we should note the article Harpum (1990), where the author investigated the issue of Liability for money laundering. To date, 3,361 scientific articles have been published in international publications, which relate to the issue of money laundering and combating this process.

The most cited work is the article Bolton and Hand (2002), which is devoted to the analysis of statistical tools for the detection of financial and cyber fraud. Ngai et al. (2011) conducted an analysis of scientific literature on the application of intellectual analysis methods to detect financial fraud, which provides a primary solution to this problem. Möser et al. (2013, September) described strategies for combating financial fraud through Bitcoin money laundering. The authors conducted a series of experiments based on reverse engineering – from the end to the beginning of the transaction. Juels et al. (2016, October) investigated the possibilities of criminal smart contracts for their application in the process of laundering criminal proceeds. Hutchings and Holt (2015) analyzed such a phenomenon as the black market economy on the Internet. The authors identified a possible criminal scenario where a black market is formed on the Internet for the sale and purchase of illegally acquired items. Colladon and Remondi (2017) revealed the importance of analyzing social media analytics to detect and counter potential financial and cyber fraud.

Despite the significant scientific work on the analyzed issue, today the research of scientific works and information requests of society regarding financial and cyber frauds, as well as the system of their countermeasures, which requires further study, is relevant. Therefore, the purpose of this article is to conduct a dynamic and bibliometric analysis of the terms that identify the system of combating financial and cyber fraud, in order to identify trends in the formation of public and scientific opinion.

2. Research Methodology and Data

We will study the system of combating financial and cyber fraud using dynamic and bibliometric analysis. Dynamic analysis is the construction of Google trends using the public web application of Google. Its main idea is to search for various terms on the global Internet based on user queries around the world. At the same time, the frequency of the searched term is determined in relation to the total volume of search requests, which are carried out in different countries of the world. Its main advantage is the dynamism associated with the determination of information at different time intervals. Also, the possibility of identifying requests by countries of the world allows you to imagine the geography of interest in the relevant topic. The results of the Google-trends analysis make it possible to form a scientifically based opinion about the current situation in society, which is related to the investigated problem.

User queries for terms such as:

- “ Fraud" for all categories, which will allow to assess the level of public interest in fraud problems;
- "Fraud" for the "Finance" category, which will contribute to the detection of fraud trends in the financial sphere;
- “Cyber Fraud” taking into account all categories to assess the level of frauds carried out in global cyberspace;
- “Cyber Fraud” for the “Finance” category, which will allow to identify fraud trends that occur in the financial sector of the country and are carried out with the help of computer technologies;
- “Money Laundering” to form an understanding of the dynamics of fraud related to the laundering of criminal proceeds and the financing of terrorism;

- "Anti-Money Laundering" and "Anti-Fraud" to assess trends in the development of systems for combating financial and cyber fraud.

These concepts will be selected for all countries of the world for the last five years, from 07.08.2017 to 07.08.2022.

Bibliometric analysis is a study of the sources of scientific literature, which is carried out using the construction and visualization of bibliometric networks implemented in the analytical package VOSviewer. The purpose of this analysis is to identify clusters of scientific publications in the world's leading publications, which are indexed in international databases, for example, Scopus or Web of Science. This contributes to the understanding of modern trends in science, the identification of relationships between the researched problem and others, and the dynamics of publishing activity. The results of the bibliometric analysis make it possible to form an opinion about the prospects and directions of further scientific research and the development of the given problem.

The array of input data was formed on the basis of queries in the Scopus database regarding the terms "Cyber Crime" and "Anti-money Laundering". As a result, two sets of data were obtained, each of which contains 2000 records of the most cited scientific publications of researchers from different countries of the world.

3. Results and Discussions

In the process of research, a dynamic analysis of the terms that identify the system of combating financial and cyber fraud was carried out using Goggle Trends. Figure 1 presents the results of the analysis of queries of Internet users for five years, who are interested in fraud in various fields, and in the financial field in particular.

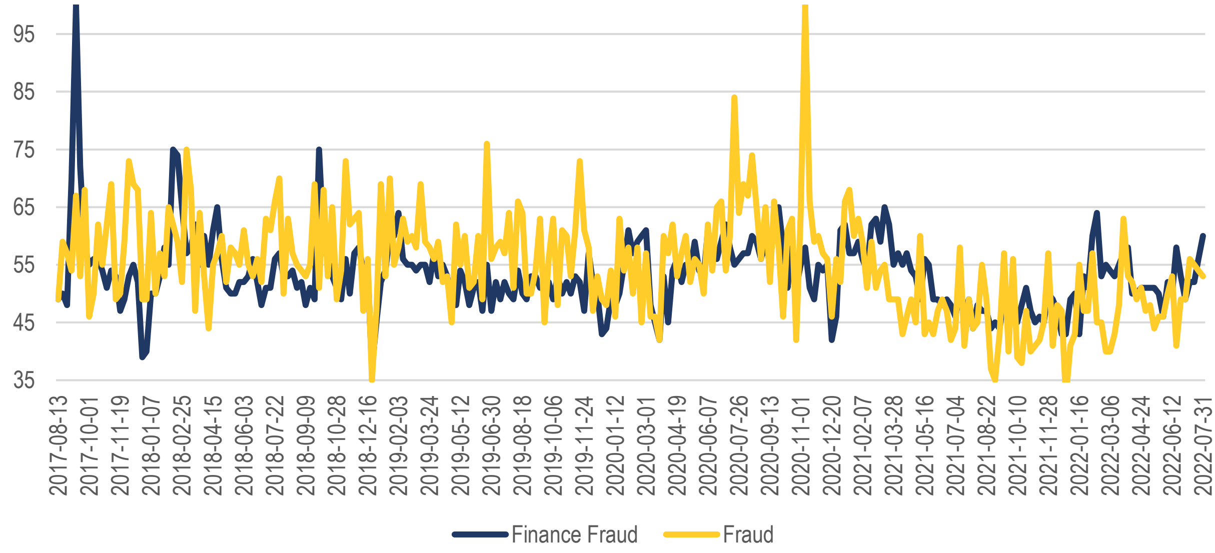

Figure 1. Dynamic analysis of user requests regarding "Fraud" and "Finance Fraud" for the period 07.08.2017 - 07.08.2022

Source: Compiled by the authors.

Large bursts of requests are observed mainly in those periods when crimes occur that have a lot of publicity or cause significant damage to society. We see that there is a slight connection between fraud and financial fraud. This confirms the value of the calculated correlation coefficient, which is equal to 0.3531. That is, 35% of frauds are financial, which may be the result of financial losses of the population as a result of certain events. Starting from the beginning of 2021, there is a trend of a slight decline in user interest in this topic. Perhaps this is due to the fact that the COVID-19 pandemic has contributed to both the growth of financial frauds and the growth of the system to combat them, or the growth of distrust of the population in financial schemes and banking transactions. As a result, this could affect the reduction of victims in the financial environment, which was reflected in the reduction of interest in this topic.

The results of the dynamic analysis of user queries regarding the terms "Fraud" and "Cyber Fraud" are presented in Figure 2.

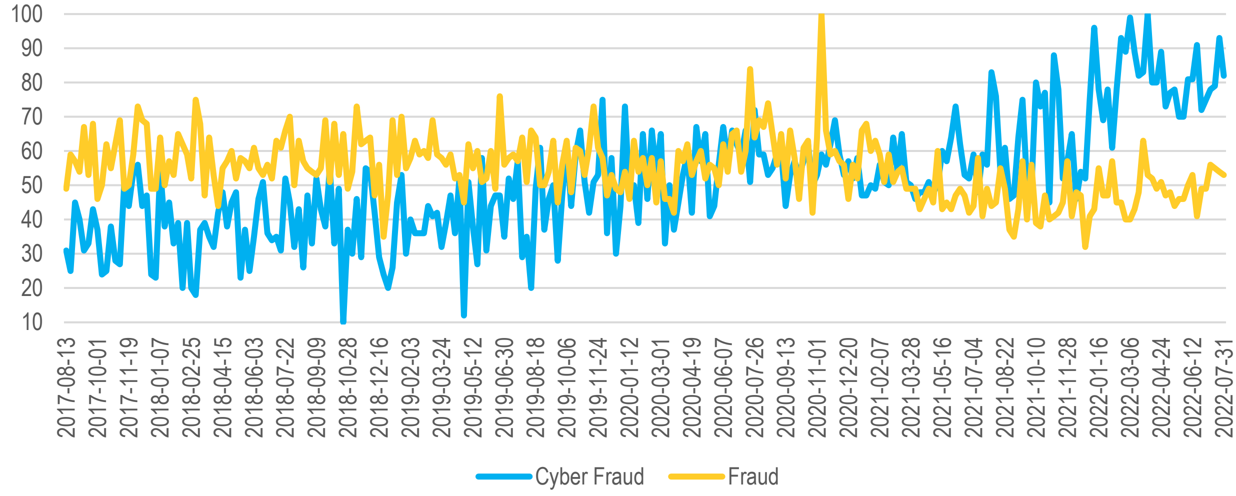

Figure 2. Dynamic analysis of user requests regarding "Fraud" and "Cyber Fraud" for the period 08/07/2017 - 08/07/2022

Source: Compiled by the authors.

It can be noted that there is a slight correlation dependence between the two data series, while it is negative. This is quite clearly traced on a stretch starting from the beginning of 2021. A series of data that reflects user inquiries about cyber fraud has a steady growing trend over five years, which may indicate a growing interest in this issue on the part of ordinary citizens. Against the background of a decrease in the number of frauds in general and financial frauds in particular, the trend of the last year and a half is positive specifically for cybercrimes. This only shows that the volume of cyber frauds that take place through the Internet and network communications is increasing, because due to the pandemic, most companies and users have transferred their business processes to the cyber environment.

What happened to cyber fraud in the financial sector? The results of the dynamic analysis (Figure 3) show that the trend of requests is rather uneven. That is, either users are interested in this topic or not. Most likely, this is due to the specificity of these frauds and their implementation to a greater extent for business entities than for individual individuals. Starting from March 2021, 3 significant spikes are visible, and in dynamics, which can be confirmed by significant events in the financial sector, which influenced the growth of interest from users of the global network.

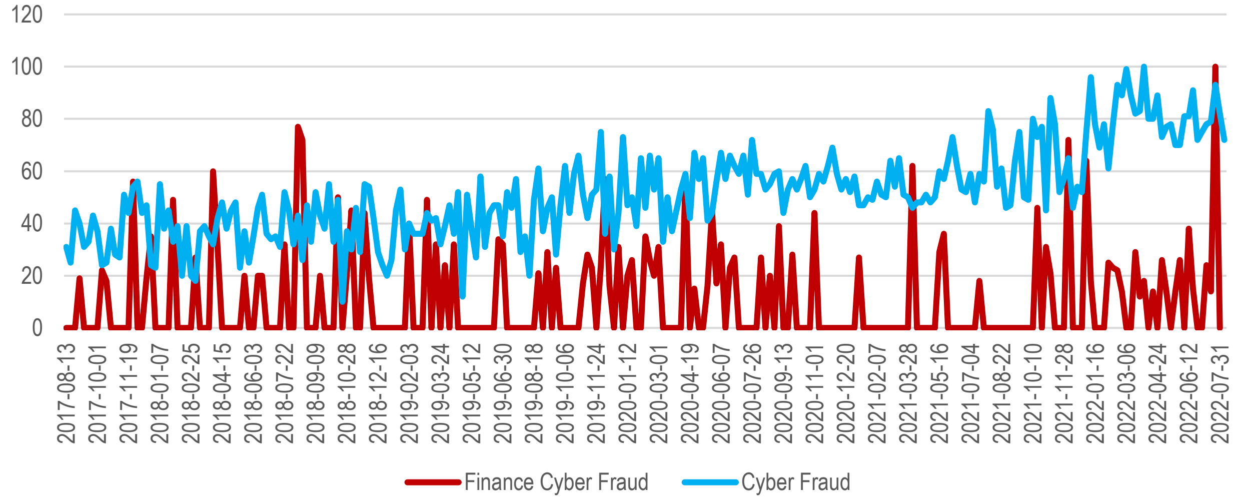

Figure 3. Dynamic analysis of user requests regarding "Finance Cyber Fraud" and "Cyber Fraud" for the period 07.08.2017 - 07.08.2022

Source: Compiled by the authors.

The results of the dynamic analysis of user queries regarding "Fraud" by geographic distribution of users are presented in Figure 4. The greatest interest in the issue of fraud occurred among the population of such countries as South Africa, Ghana, Great Britain, the USA, Canada, Ireland, Cyprus, Australia, Singapore , UAE. The represented countries belong to countries with different levels of economic development, and the difference between them is quite significant. Such a situation may indicate that the least developed countries are more favorable for the legalization of proceeds obtained through crime. As for developed countries, users from there face more fraud because they have a high level of financial income.

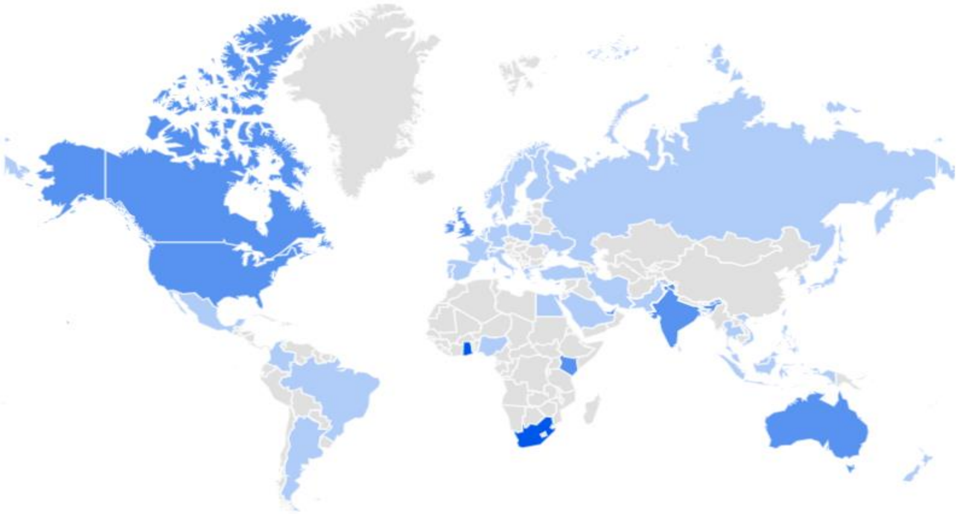

Figure 4. Dynamic analysis of user requests regarding "Fraud" by geographical distribution in the period 08/07/2017 - 08/07/2022

Source: Compiled by the authors.

The results of the dynamic analysis of user requests regarding "Finance Fraud" by geographic distribution (Fig. 5) are similar to the previous findings. Representatives of such countries as the Republic of South Africa, Great Britain, Saint Helena Island, USA, Ireland, Canada, Australia, New Zealand, Singapore, Ghana are most interested in the problem of financial fraud. That is, the trend is characteristic of a number of countries that differ radically in terms of different levels of economic development.

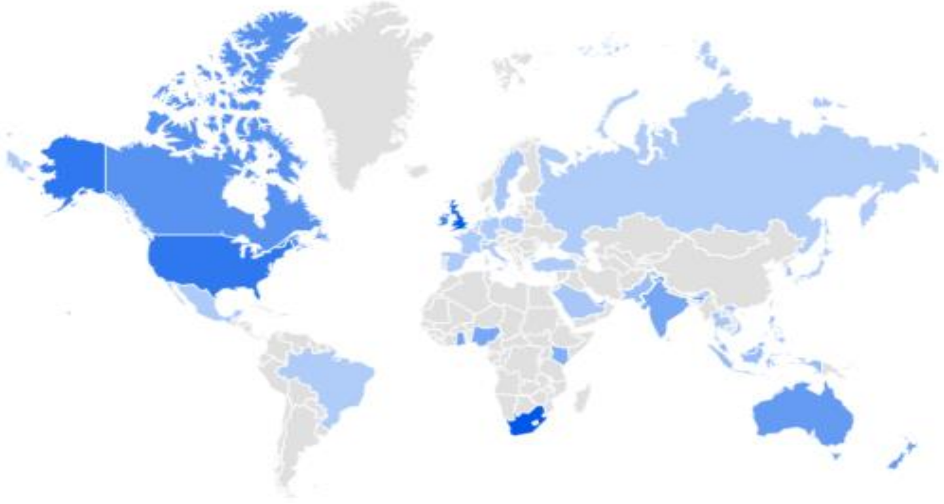

Figure 5. Dynamic analysis of user requests regarding "Finance Fraud" by geographic distribution in the period 08/07/2017 - 08/07/2022

Source: Compiled by the authors.

As for the dynamic analysis of user requests regarding “Finance Cyber Fraud” and “Cyber Fraud”, the results were not pronounced. This is due to the fact that a small number of requests are received from different countries, so it is difficult to detect the geography of their distribution.

A dynamic analysis was also carried out for the concept of “Anti-fraud” in order to determine the trends in the formation of the anti-fraud system. Its results compared to user queries on fraud are presented in Figure 6. It can be seen that there is no relationship between data on fraud and countermeasures. The presented trends characterize the process as chaotic. Perhaps their further research will reveal the dependence on lag. This would indicate that the surge in interest in fraud, generated by massive hacking attacks, over time also affects the surge in interest in countermeasures.

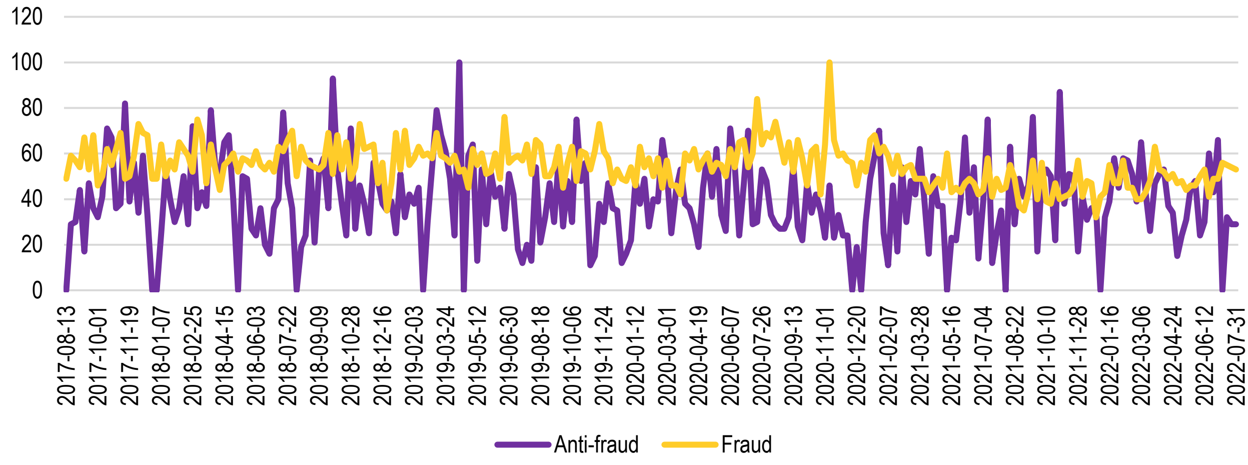

Figure 6. Dynamic analysis of user requests regarding "Fraud" and "Anti-fraud" for the period 08/07/2017 - 08/07/2022

Source: Compiled by the authors.

The increase in the frequency of use of electronic financial systems and the development of electronic funds have increased the interest of criminals in fraud in the financial sphere. This is especially relevant for criminals whose activities are related to the laundering of illegal funds. So, Goggle Trends confirm that interest in financial crimes fluctuates over five years and does not reach zero level (Fig. 7). There is also a slight upward trend since the beginning of 2021. Fluctuations, as with fraud in general, depend on the level of publicity and scale of the fraud. A significant observation is that, after all, there is significant interest in anti-money laundering systems to a greater extent than interest in the money laundering process itself. In our opinion, this is a rather positive fact, which indicates the strengthening of measures against the legalization of funds in accordance with the requirements of international organizations.

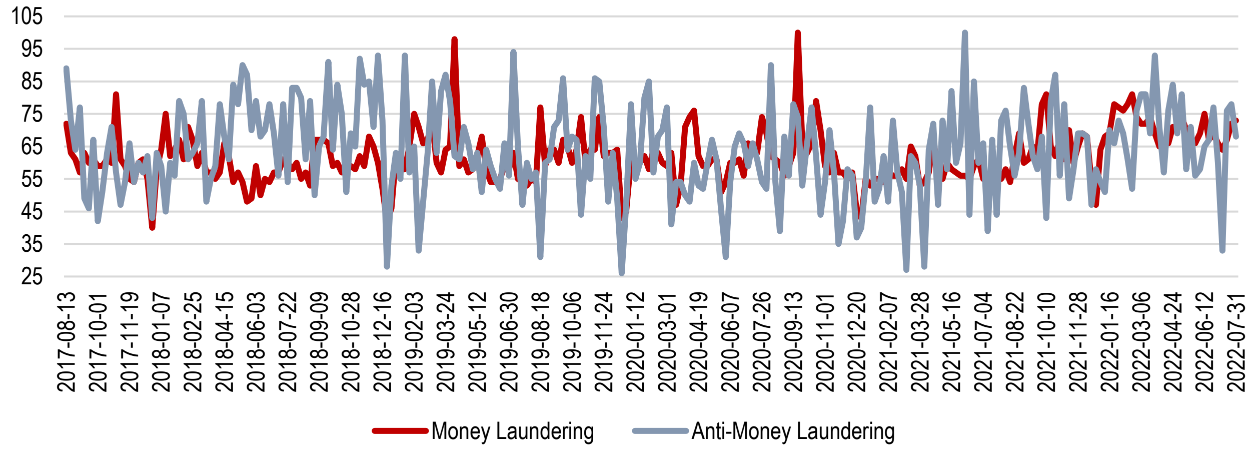

Figure 7. Dynamic analysis of user requests regarding “Money Laundering” and “Anti-Money Laundering” for the period 07.08.2017 - 07.08.2022

Source: Compiled by the authors.

In the course of the research, a bibliometric analysis of scientific publications selected from the Scopus database was carried out. Figure 8 shows a map of keywords in the authors' research in the section “Cyber Crime”. “Cyber Crime” was used as a synonym for “Cyber Fraud” because more publications were found with this term. After studying the keyword map, you can see that the ten most powerful clusters of scientific works have been formed. The largest red cluster reflects research in the field of cyber fraud, which is more related to the tools for their detection. That is, these are publications on machine and deep learning, the method of support vectors, decision trees, Data Mining, clustering, classification, machine learning techniques, neural networks, logistic regression, etc. Next is the green cluster, which characterizes a more general direction that deals with concepts related to information and cyberspace. These are cyber security, cyber war, cyber fraud, cyber crime, Internet crimes, security, investigation, etc. The blue cluster reflects research related to network aspects of countering cyber fraud, namely, network protocols, network traffic, network security, network forensics, internet protocols, intrusion detection, etc. The yellow group corresponds to the direction of digitization and digital forensics: digital forensics, digital devices, digital evidences, digital storages, cellular telephones, communication, etc. The lilac cluster reflects the direction of cyber protection, blue - data protection, orange - data authentication and encryption, brown - Internet of Things, beige - social networks, pink - computer crimes.

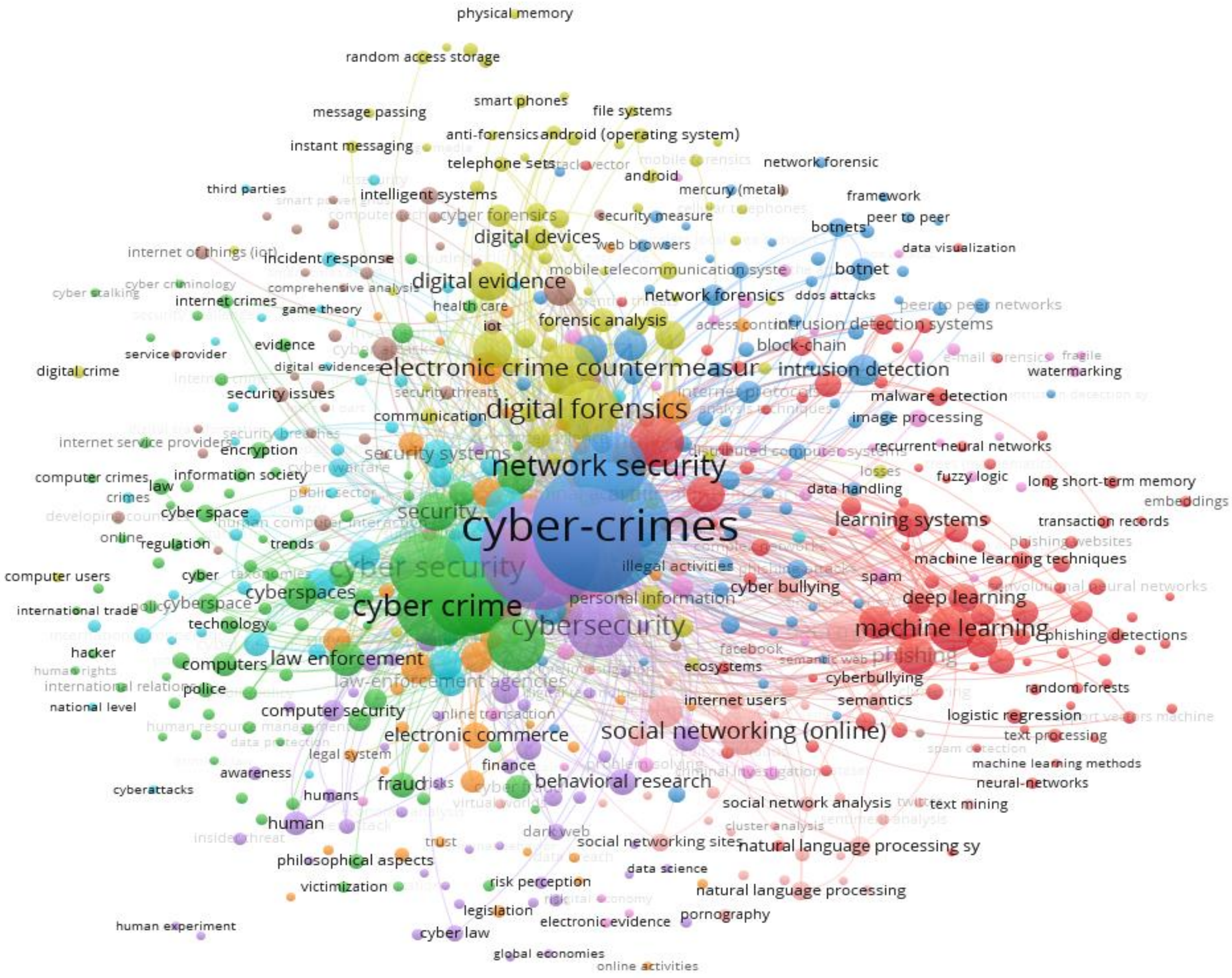

Figure 8. Map of keywords in the authors' research in the section "Cyber Crime"

Source: VOSviewer.

If you look at the keyword map by year (Fig. 9), you can see that in 2014, cybercrimes were most associated with the Internet, network protection, and digital devices. During 2015 - 2017, the trend changed towards research of the general direction and network aspects of cyber fraud. Whereas, since 2020, the most significant connection has been observed with cybercrime countermeasures, namely machine learning. It can be concluded that the growing level of cyber fraud requires the use of progressive and effective methods than before. Therefore, scientific teams are engaged in the development of effective tools for combating cybercrimes, which are used to quickly detect an attack or data leak, complicate user identification and verification processes, predict possible hacker attacks, and create portraits of potential victims of cybercrimes and cybercriminals themselves.

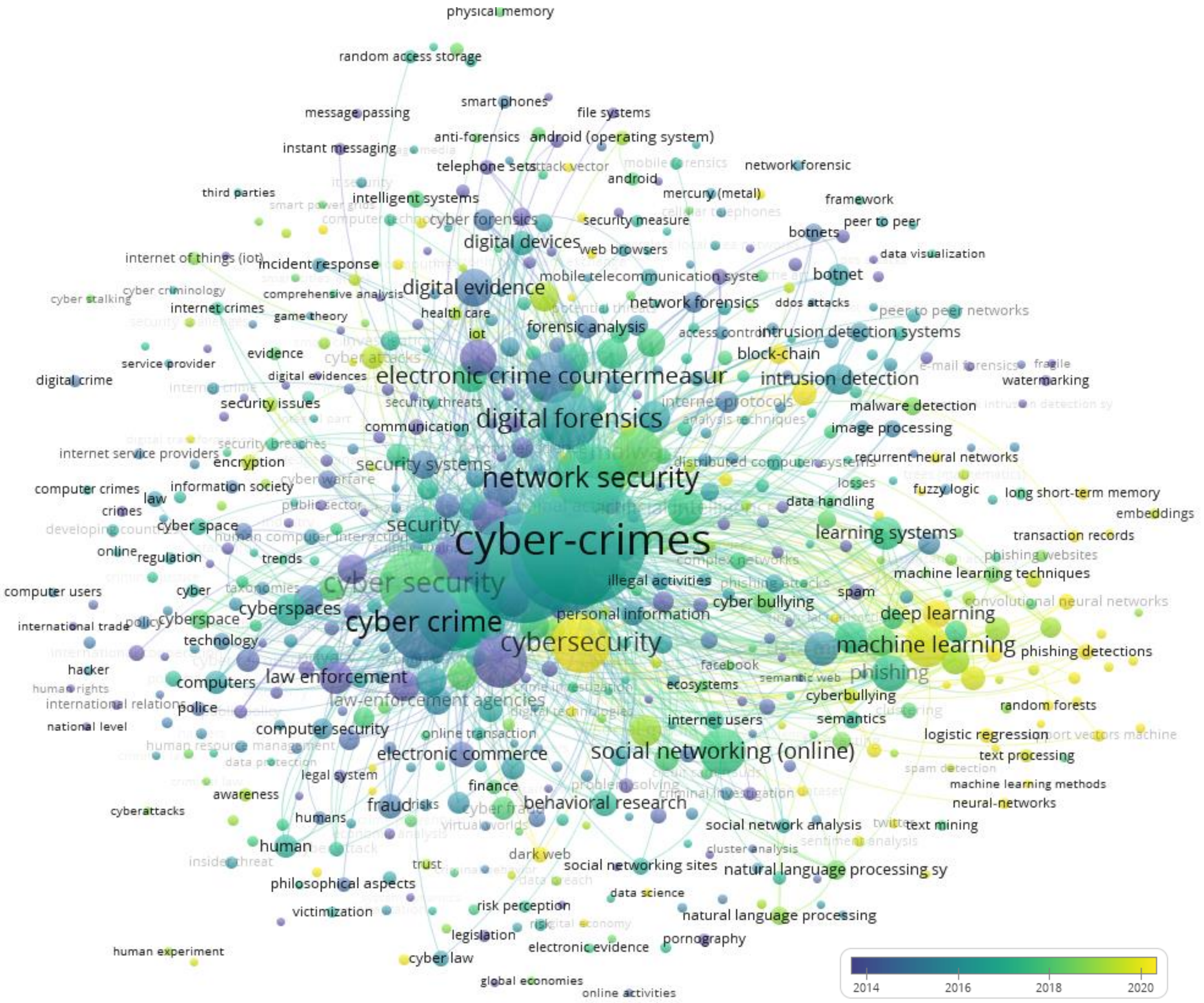

Figure 9. Map of keywords in the authors' research in the section "Cyber Crime" by year

Source: VOSviewer.

The map of keywords in the section "Money Laundering" shows the presence of 8 clusters (Fig. 10). The largest is the red cluster, the direction of which is related to mathematical methods and information technologies in the financial sphere. Here you can highlight concepts that reflect artificial intelligence, learning systems, machine learning, social networking, data mining, laundering, finance, financial institution, etc. The green cluster refers to the direction of cryptocurrencies, bitcoins and blockchains. The blue cluster is associated with legislation in the field of money laundering, bribery, drug trafficking, and organized crime. The yellow cluster covers the direction of corruption and related tax evasion, shadow economy, and financial crimes. The lilac cluster reveals the concept of financial terrorism. The smallest blue sector covers the direction of FATF international requirements, orange - the financial services sector, brown - financial institutions.

After examining keywords by year (Fig. 11), it can be observed that in the last three years, money laundering and financial crimes are more closely related to cryptocurrencies and blockchains. Machine learning and automatic crime detection methods are used to counter the legalization process. This is explained by the increasing role of electronic money and financial instruments in modern life and the emergence of new opportunities for cybercriminals. Figure 11 also shows that the majority of publications relate specifically to the types of processes of laundering criminal proceeds. The peak of this kind of research came in 2018.

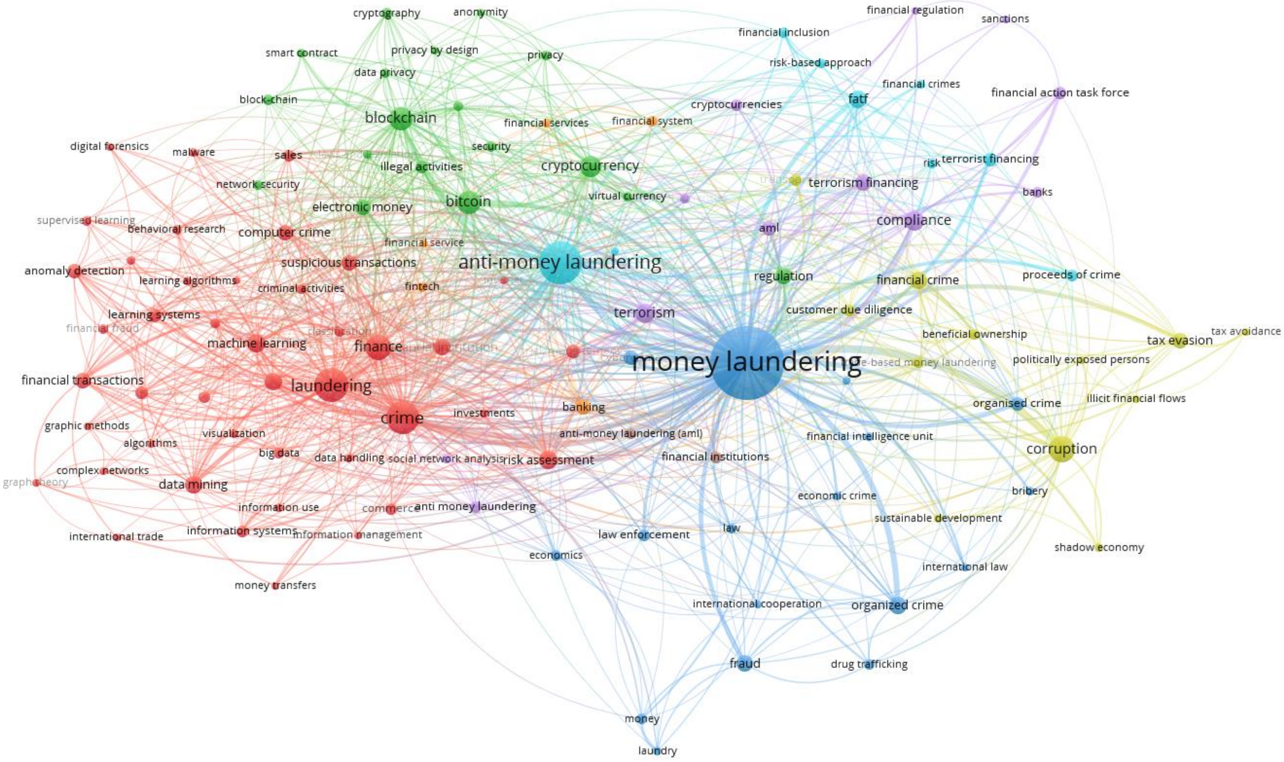

Figure 10. Map of keywords in the authors' research in the section "Money Laundering"

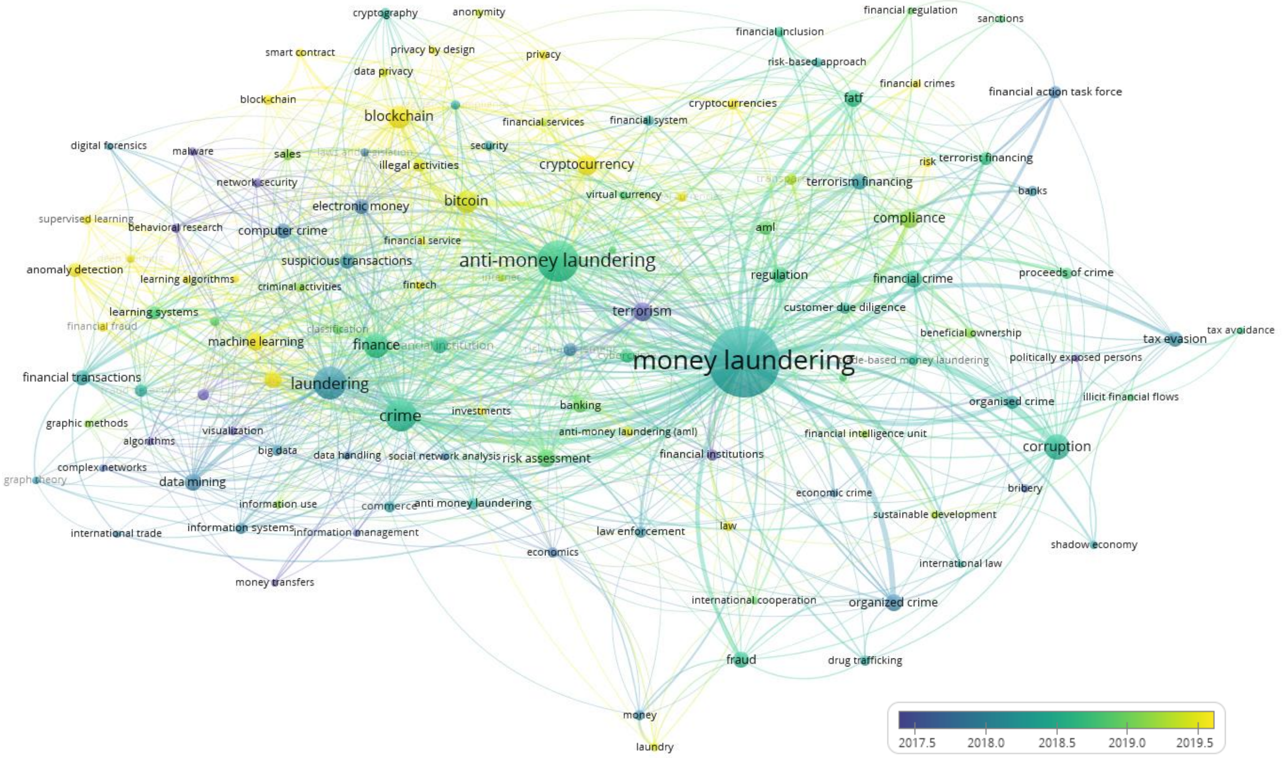

Figure 11. Map of keywords in the authors' research in the section "Money Laundering" by year

Source: VOSviewer.

Conclusion

The consequences of the Fourth Industrial Revolution caused a rapid development of information and communication systems and technologies in various spheres of society's life. This led to the appearance of cybercrimes, the main purpose of which is related to illegally obtaining access to the personal data of certain individuals and company databases. Among them, financial cybercrimes have gained popularity, the implementation of which is connected with the laundering of funds obtained as a result of criminal activities and the financing of terrorism. Based on this, the conduct of this study was related to the identification of trends in society and the scientific community regarding the formation of a system for combating financial and cyber fraud. It was carried out with the help of dynamic analysis of user requests for the main terms that identify the countermeasure system, based on Google trends. A bibliometric analysis of the most cited scientific works on the subject under study was also conducted using the VOSviewer analytical package.

The results of a dynamic analysis of Internet users' requests for five years showed that 35% of frauds are financial. Although there has been volatility in inquiries regarding "Fraud" and "Finance Fraud", since the beginning of 2021 their volumes have slightly decreased compared to previous years. A possible reason was the global pandemic, which contributed to the increased attention of the population to their own finances. Another trend was found in cyber fraud. The dynamics of requests for this term showed a gradual growth over five years. At the same time, since the beginning of 2021, their number has significantly exceeded fraud inquiries. This confirms the conclusions of the impact of the pandemic. As many individuals and companies have switched to remote work, this has resulted in increased attention from hackers and cyber-swindlers. Although the analysis of "Finance Cyber Fraud" showed the least interest from users, the observed jumps are in line with the trend shown by queries about "Cyber Fraud".

The results of a dynamic analysis of user requests for "Fraud" and "Finance Fraud" by geographic distribution showed that they aroused interest among the population of countries with a significant difference in economic development, that is, least developed and highly developed countries. On the one hand, this can be explained by the fact that representatives of poor countries are potential cyber fraudsters, and developed countries are potential victims of fraud.

The conducted bibliometric analysis of scientific publications in the section "Cyber Crime" made it possible to obtain ten clusters that reflected the following established areas of research issues: toolkit for detecting cyber fraud, formation of general concepts, network aspects of countering cyber fraud, digitization and digital forensics, cyber protection, data protection, authentication and encryption data, Internet of things, social networks, computer crimes. Today, the focus of research is shifting towards methods of countering cybercrimes. The constructed map of keywords in the section "Money Laundering" made it possible to identify 5 large and 3 small clusters. These groups reflect such directions as mathematical methods and information technologies in the financial sphere, cryptocurrencies and blockchains, legislation in the sphere of money laundering, corruption, financial terrorism, financial services and institutions, international FATF requirements. Over the past three years, the direction of potential money laundering through cryptocurrencies and blockchains has been the most studied.

The obtained results of this study can be useful in the process of forming a strategy to combat financial and cybercrimes at the state level, and will also contribute to the formation of an analytical basis for the scientific community and practitioners.

Author Contributions: Conceptualization, Yarovenko, H. and Rogkova, M.; **methodology**, Yarovenko, H. and Rogkova, M.; **software**, Yarovenko, H. and Rogkova, M.; **validation**, Yarovenko, H. and Rogkova, M.; **formal analysis**, Yarovenko, H. and Rogkova, M.; **investigation**, Yarovenko, H. and Rogkova, M.; **resources**, Yarovenko, H. and Rogkova, M.; **data curation**, Yarovenko, H. and Rogkova, M.; **writing-original draft preparation**, Yarovenko, H. and Rogkova, M.; **writing-review and editing**, Yarovenko, H. and Rogkova, M.; **visualization**, Yarovenko, H. and Rogkova, M.; **supervision**, Yarovenko, H. and Rogkova, M.; **project administration**, Yarovenko, H. and Rogkova, M.

References

1. Bequai, A. (1998). Guide to cyber-crime investigations. *Computers and Security*, *17*(7), 579 – 582. [Link]

2. Benjamin, R., Gladman, B. and Randell, B. (1998). Protecting IT Systems from Cyber Crime. *Computer Journal*, *41*(7), 429 – 443. [Link]

3. Bolton, R. J. and Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical science*, *17*(3), 235 – 255. [Link]

4. Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, *30*(8), 719 – 731. [Link]

5. Colladon, A. F. and Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications*, 67, 49 – 58. [Link]

6. FATF (2001). *The FATF Recommendations*. [Link]

7. Feily, M., Shahrestani, A., and Ramadass, S. (2009, June). A survey of botnet and botnet detection. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, 268-273. [Link]

8. Harpum, C. (1990). Liability for money laundering. *The Cambridge Law Journal*, *49*(2), 217 – 220. [Link]

9. Huang, Q., Singh, V. K. and Atrey, P. K. (2014, November). Cyber bullying detection using social and textual analysis. In Proceedings of the 3rd International Workshop on Socially-Aware Multimedia, 3-6. [Link]

10. Hutchings, A. and Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596 – 614. [Link]

11. IBM (2022). How much does a data breach cost in 2022? [Link]

12. Juels, A., Kosba, A. and Shi, E. (2016, October). The ring of gyges: Investigating the future of criminal smart contracts. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 283-295. [Link]

13. Kolodenker, E., Koch, W., Stringhini, G. and Egele, M. (2017, April). Paybreak: Defense against cryptographic ransomware. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 599-611. [Link]

14. Möser, M., Böhme, R. and Breuker, D. (2013, September). An inquiry into money laundering tools in the Bitcoin ecosystem. In *2013 APWG eCrime researchers summit*, 1-14. Ieee. [Link]

15. Mumford, E. (1998). Problems, knowledge, solutions: Solving complex problems. *Journal of Strategic Information Systems*, *7*(4), 255 – 269. [Link]

16. Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y. and Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems*, *50*(3), 559 – 569. [Link]

17. OAS (1994). The Council of Europe Convention on Cybercrime: status quo and future challenges. Retrieved from August 1, 2022. [Link]

18. Ruan, K., Carthy, J., Kechadi, T. and Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation*, *10*(1), 34 – 43. [Link]

19. Tounsi, W. and Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers and Security*, 72, 212 – 233. [Link]