DOI: 10.55643/fcaptp.5.46.2022.3897

RECENT TRENDS IN THE FINANCIAL CRIME OF THE WORLD

Katarina Sigetova
PhD student, University of Economics in Bratislava, Bratislava, Slovakia;
ORCID: 0000-0002-7058-3681

Lenka Uzikova
PhD student, University of Economics in Bratislava, Bratislava, Slovakia;
ORCID: 0000-0002-5700-1026

Tetiana Dotsenko
PhD in Economics,
Technical University of Berlin, Berlin, Germany; Sumy State University, Sumy, Ukraine;
e-mail: t.dotsenko@uabs.sumdu.edu.ua
ORCID: 0000-0001-5713-2205
(Corresponding author)

Anton Boyko
D.Sc. in Economics, Professor,
Sumy State University, Sumy, Ukraine;
ORCID: 0000-0002-1784-9364

Received: 12/09/2022
Accepted: 24/10/2022
Published: 31/10/2022

ABSTRACT

The paper emphasizes that the digitalization of the modern world, the development of information technology, the spread of the Internet, computer networks, and the use of cyberspace have facilitated the daily life of society. However, these factors have entailed a threat to the security and confidentiality of information, personal data, and the financial system. The authors state that financial fraud is becoming an increasingly severe global problem since criminals use the financial ecosystem for money laundering and illegal financial transactions. The study's primary purpose is to identify the latest trends in the financial crime of the world. The methodological tools of the research consisted of theoretical research methods (grouping, abstraction), empirical research methods (observation, description), and the resource base of the information platform, bibliometric analysis, and modeling. The following scientific categories were chosen as the objects of study: regulatory and legal aspects of financial crimes, online crimes and cybercrimes, methods and systems of regulation, control, prevention, counteraction, combating financial crime, and modeling of financial crime processes. The paper analyzes the literature sources regarding the shift of the interest of modern financial market scientists to the study of the features of financial crime. The relevance of identifying the latest trends in financial crime lies in the fact that the study of financial crime trends will allow the improving of the awareness of financial fraud, creating common databases, building coalitions, and identifying effective and efficient ways to improve the ability to combat financial crime at a more effective national and global level. At the initial stage of the work, a bibliometric analysis of scientific publications dedicated to the study of the latest trends in financial crime was carried out. As a result, literary works for the study of the specified issue were systematized; a map of relationships between key terms and other scientific concepts was created; a content-contextual and intercluster analysis of the obtained blocks of bibliometric analysis was carried out; a map of the relationships of the studied key concepts with other scientific categories in dynamics was constructed and the contextual-time block was analyzed. The research in this paper is carried out in three parts, which provide for the definition of several research vectors. As a result of research - the authors discuss potential sources and tools of financial fraud with their negative, harmful aspects for identification, in-depth consideration, and study; they identify tools for countering financial crimes; practical models for evaluating, analyzing, identifying, comparing, and visualizing the features of financial crime are described. The conclusion of the study assumes that the results of the study can be practically applied by financial organizations, institutions, and business entities for the future safe functioning of the financial sector but taking into account the need for constant development of IT support for financial transactions as a response to the rapidly changing needs of our time.

Keywords: financial crimes, cybercrime, money laundering, risky financial transactions, cyber security, financial crime modeling

JEL Classification: K00, K22, G24

INTRODUCTION

Digitalization of the modern world, the development of information technologies, and the spread of the Internet, computer networks, and cyberspace form the basis of contemporary society. All these latest measures have made everyday life easier for society, but they threaten the security and confidentiality of information, personal data, and the

financial system. Financial fraud is becoming an increasingly serious global problem, as the financial ecosystem is now seen as a complex network of institutions, operations in different volumes, currencies, values, from different territorial locations, using different tools, in which financial institutions have built and grouped a range of products and services taking into account the advantages of globalization, digitalization and opportunities of high financial complexity, which is also used by the criminal world for money laundering and illegal financial transactions.

Financial crime is multi-faceted, multi-aspect, national, geographically unlimited, and often invisible, hindering its identification, analysis, evaluation, and fight against it. Negative consequences of financial crimes affect many areas. Institutions, organizations, corporations, and individuals incur significant financial costs to prevent illegal financial transactions. However, despite these measures, illegal funds continue circulating in the financial system, causing huge losses in business and a tax gap, affecting the country's economy, infrastructure, and the well-being of the population. In turn, this causes destabilization of the national system through criminal, fraudulent activities financed by financial criminals.

Therefore, studying trends in financial crime is now a particularly relevant issue. This will help to increase awareness of financial fraud, create common databases, form coalitions, and identify efficient ways to improve the ability to combat financial crimes at the national and global levels.

LITERATURE REVIEW

The analysis of literary sources proves that the interest of modern financial market scientists is shifting to the study of the features of financial crime. In terms of the regulatory and legal aspects of financial crimes, modern specialists have covered the following issues over the past year: determining the impact of illegal financial flows in terms of the illegal use of public funds on the right to development, based on criminal court documents – Agbor A. A. [1]; description of the analysis of the factors that determine the collection of information through whistleblowers about potential financial crimes, potential complaints, and relevant referents that affect the formation of controls that complement the theoretical legislative criminal base of financial offenses – Sallaberry J. D., Flach L. [50]; study of the framework of financial behavior for the prevention of financial abuse through market regulators – Klimczak K. M., Sison A. J. G., Prats M., Torres M. B. [21]; coverage of data protection rules applicable to financial intelligence units – Quintel T. [44]; study of financial and economic security through criminal policy – Oliinyk O. S., Shestopalov R. M., Zarosylo V. O., Stankovych M. I., Golubytskyi S. G. [41]; description of interaction strategies for e-commerce businesses in the online world - Jenjira Phomkamin, Chalita Pumpuang, Pattarawan Potijak, Supaporn Sangngam, Issariya Ketprasit, Bahaudin G. Mujtaba [18]; analyz corporate behavior in digital technologies - Skrynnyk, O. [54]; consideration of the features of the banking sector - Agnihotri A., Gupta S. [2], Zarutska E., Pavlova T., Sinyuk A. [61], Buriak A., Lyeonov S., Vasylieva T. [12], Meresa M. [36], Morsher Ch., Horsch A., Stephan J. [37]; underlining the corruption of the legislative framework - Bozhenko, V., Kuzmenko, O. [10], Juarez-Garcia M.I. [19], Kaya H.D., Engkuchik E.N.S. [20]; other modern socio-economic orders - Rubanov P., Lyeonov S., Bilan Y., Lyulyov O. [48], Louis R. [31], Bouchetara M., Nassour A., Eyih S. [9], Al-Khonain S., Al-Adeem K. [4], Levchenko V., Boyko A., Savchenko T., Bozhenko V., Humenna Yu., Pilin, R. [27], Formankova S., Trenz O., Faldik O., Kolomaznik J., Vanek P. [14], Samoilikova A., Kunev R. [51], Boronos V., Zakharkin O., Zakharkina L., Bilous Y.[8], Lyulyov O., Paliienko M., Prasol L., Vasylieva T., Kubatko O., Kubatko V. [32], Kuzmenko O., Lieonov S., Kashcha M. [24].

In recent years, special attention has also been paid to cybercrime. Thus, Li M. [28] highlights the results of a study on the illegal use of Ethereum blockchain technology; Singh V., and Sharma S. K. [53] describe the application of blockchain technology in the food industry; Trozze A., Kamps J., Akartuna E. A., Hetzel F. J., Kleinberg B., Davis T., Johnson S. D. [57] study the features of cryptocurrencies and predict future financial crimes; Kuzmenko O. V., Kubálek J., Bozhenko, V. V., Kushneryov O. S. and Vida I. [23] reveal an approach to innovation management to protect the financial sector from cybercrime; Pandey A. B., Tripathi A., Vashist P. C. [43] investigate cybersecurity trends, new technologies, and threats; Bulut H. and Kacar F. [10] reveal the features of preventing cyber-attacks on SCADA systems used in the financial sector; and others; Stavrova E. [55], Rizk S. [45], Zatonatska T., Hubska M., Shpyrko V. [62] - banks' Digital Challenges; Muradov İ. [38] identify e-governance issues; Baltgailis J., Simakhova A. [6] - threats to the Technological Innovations of Fintech Companies; Oloveze A.O, Ugwu P.A., Okonkwo R.V.O., Okeke V.C., Chukwuoyims K., Ahaiwe E.O. [42] describe m-health innovation; and others.

The analysis of literature also shows that the efforts of modern scientists are aimed at developing methods and systems for regulation, control, prevention, counteraction, and fights against financial crime, namely: Müller W., Mühlenberg D., Pallmer D., Zeltmann U., Ellmauer C., Demestichas K [39] use knowledge engineering and ontology for crime investigation; Rose K. J. [47] determines the effectiveness of EU regulation on money laundering in terms of introducing restrictions on the use of tax havens; Wang S., Zhu X., And Zhang B. [58] investigate the financial crime in terms of financing the

proliferation of weapons of mass destruction and suggest appropriate countermeasures; Mahi-Al-rashid A., Hossain F., Anwar A., Azam S. [34] suggest detecting a false data attack in a smart network using prediction; Yeh S. S. [60] considers new OSCE recommendations on combating corruption, money laundering, and terrorist financing;Gupta A., Mishra M. [17] describe aspects of the use of artificial intelligence; Taghieva T., Tiutiunyk I. [56] summarize innovative, economic and marketing determinants of financial security; Antonyuk N., Plikus I., Jammal M. [5] determine ways to ensure the quality of human capital in the conditions of digital transformation; Leonov S., Yarovenko H., Boiko A., Dotsenko, T. [26] offer a prototype of information system automation for monitoring banking transactions related to money laundering; Serpeninova Yu., Makarenko I., Plastun A., Babko A., Gasimova G. [52], Lyeonov S. , Kuzmenko,O. , Yarovenko H. , Dotsenko T. [26, 25] - other innovative financial instruments.

Another essential aspect is modeling financial crime processes. Thus, Lin K. and Gao Yu [29] describe the interpretability of the financial fraud detection model using the SHAP group; Granados O. M. and Vargas A. [16] suggest assessing the mechanism of money laundering in financial networks using topological and geometric considerations; Gerbrands P., Unger B., Getzner M., and Ferverda J. [15] consider the effect of anti-money laundering policies through empirical network analysis (network analysis model); Rocha-Salazar J., Segovia-Vargas M., Camacho-Miñano M. [46] describe modeling the detection of shell companies in financial institutions using the dynamic social network; Maçãs C., Polisciuc E., Machado, P. [33] suggest visualization simulations for detecting financial fraud using the ATOVis tool; Djamila T.A., Abdelatif M. [13] - count the Impact of Setting up a Cloud Computing Solution; Lopez B.S., Caetano I.M.S., Alcaide A.V. [30] conduct a risk assessment of social networks; Naseer M.M., Guo Y., Zhu X. [40], Alikariev O.F.U., Poliakh S. [3] - description of empirical assessment of impact factors; Matvieieva Yu., Hamida H.B. [35] - modelling and Forecasting the Human Health; Kuzmenko O. V., Koibichuk V. V. [22], Rubanov, P., Vasylieva, T., Lyeonov, S., & Pokhylko, S. [48], Yarovenko H., Bilan Y., Lyeonov S., Mentel G. [59], Berzin P. , Shyshkina O., Kuzmenko O., Yarovenko H. [7] - other important techniques for modeling financial processes.

Analysis of the latest trends in financial crime indicates significant scientific achievements in certain areas of the issue under consideration. Therefore, their in-depth study is an essential task for developing further recommendations.

AIMS AND OBJECTIVES

The study's primary aim is to identify the latest trends in the financial crime of the world.

METHODS

The methodological tools of the research consisted of theoretical research methods (grouping, abstraction), empirical research methods (observation, description), and the resource base of the information platform, bibliometric analysis, modeling.

The use of mutually determined theoretical research methods, such as grouping and abstraction, provided the possibility of unifying the researched scientific concepts, such as "financial crimes, cybercrimes, money laundering, risky financial transactions, cyber protection, modeling of financial crime", according to different directions, according to the relevant signs; prepare the basis for further generalization. Empirical methods of research - observation and description provided a better, more thorough understanding of the practical experience of the problem of financial crime, ways of solving it. Part of the results is presented by modeling financial crime processes. The use of the resource base of the information platform allows you to research, analyze, systematize literary assets, and implement a bibliometric analysis.

To study the development of world scientific opinion in the direction of studying the trends of financial crime, it is advisable to first conduct a bibliometric analysis of the data of scientific assets, which can be implemented on the Scopus database, by using the VOSViewerv.1.6.15 toolkit. The initial stage of the bibliometric analysis of the published scientific treatises of the Scopus database for a certain period of time was the creation of a map of relationships between the key terms "financial crimes, cybercrime" and other scientific concepts. The resulting map shows that the system selected the concepts most closely related to the studied categories. These concepts are grouped into clusters of interrelated scientific terms, represented by different colors. Moreover, scientific categories are represented by circles of different sizes: larger circles mean a higher number of mentions of the category in studies of such a scientific concept, which is located in it, as a key concept that is interconnected with the researched concepts of "financial crimes, cybercrime". There are certain intersections between the selected clusters, which indicates the interconnectedness of these scientific categories. To study the evolutionary-temporal perspective of the research, a map of the relationships of the researched key concepts "financial crimes, cybercrime" with other scientific categories for a certain period of time in dynamics is built, the analysis of the contextual-

DOI: 10.55643/fcaptp.5.46.2022.3897

temporal block of bibliometric analysis is carried out. The result is the grouping of important determinants of the analysis of financial crime trends in different periods of time, using different saturation of colors, that is, from early publications to modern ones.

RESULTS

Analysis of the resulting map of relationships between the key terms "financial crimes, cybercrime" and other scientific concepts, obtained at the initial stage of bibliometric analysis, shows that the system selected 160 concepts most closely related to the studied categories. These concepts are grouped into 8 clusters of interrelated scientific terms (Figure 1), which are visually represented by different colors: 32 concepts are depicted in red, 31 concepts in green, 22 concepts in blue, 21 concepts in yellow, 18 concepts in purple, 14 concepts - blue, 13 concepts - yellow-hot, 9 concepts brown.

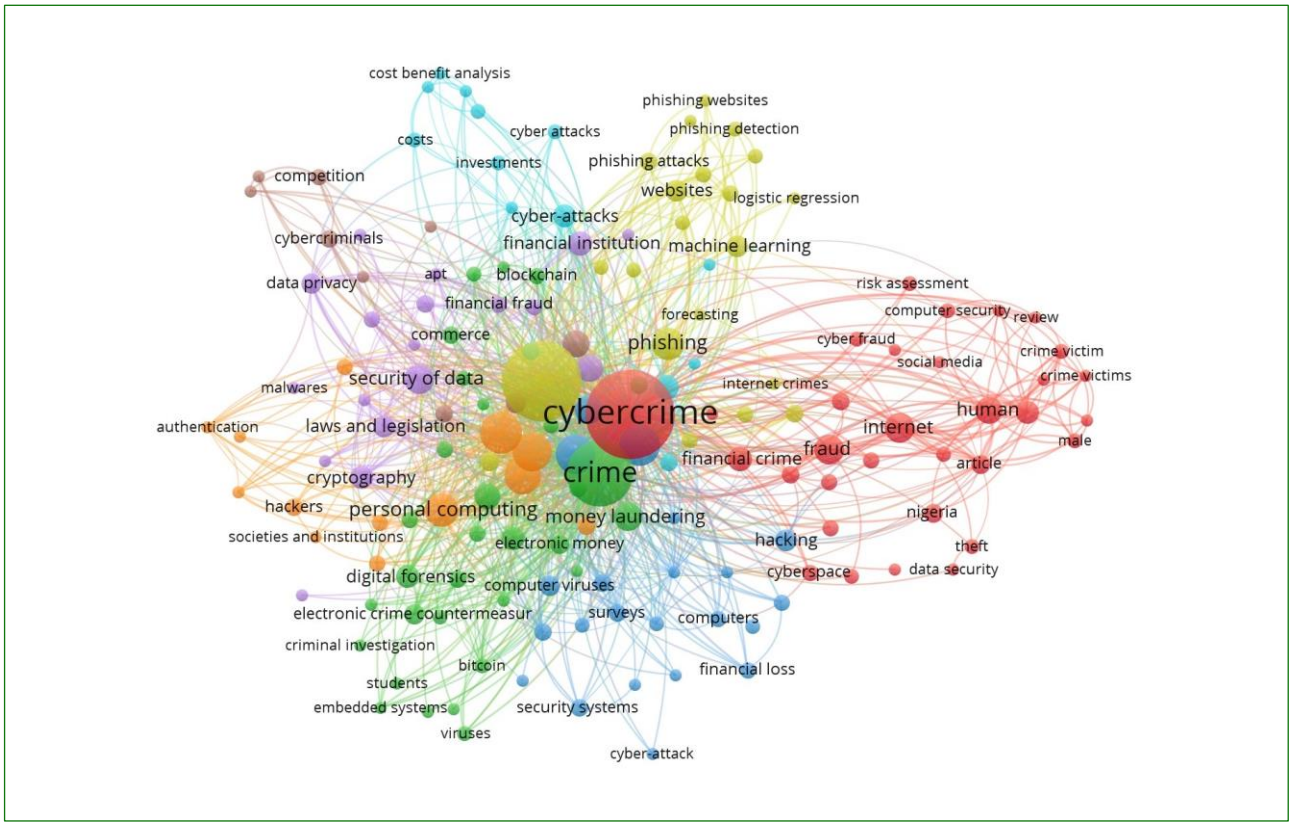

Figure 1. Scientific bibliography of the concepts of "financial crimes, cybercrime" for the period 2012-2022 using software tools.
(Sources: developed/compiled/systematized by the authors based on the Scopus database using the VOSViewerv.1.6.15 software toolkit (Dotsenko, 2022)

Thus, while conducting a content-contextual analysis of the obtained blocks of bibliometric analysis, we note that the largest circle sizes, that is, the highest, fundamental influence in the study of "financial crimes, cybercrime" issues, have the following categories: "phishing" - detection of phishing sites and prevention of phishing attacks (yellow block), "digital forensics" - electronic forensics, countermeasures, investigation of fraud (green block), "cybersecurity" - ensuring cyber security, mobile security (blue block), "network security" - organization of security of personal computers, network security (yellow-hot block), "security of data" - formation of information protection, confidentiality and data preservation (purple block), "economic impacts" - financial and economic consequences of cyber-attacks, investments and costs (turquoise block).

Intersections between selected clusters indicate a certain interrelationship between the relevant scientific categories: phishing sites, unprotected networks, the Internet, and cyberspace are platforms for the activities of financial cybercriminals; digital information and databases are the basis for the implementation of criminal actions; cybercrimes entail significant financial losses; in turn, the effective work of digital forensics contributes to the disclosure of cybercrimes and the prosecution of financial fraudsters; a proper system of protection, cyber security, mobile security, makes it impossible for fraudsters to commit illegal actions.

The result of the study of the evolutionary-time perspective of the research is the construction of a map of the relationships of the studied key concepts "financial crimes, cybercrime" with other scientific categories for the period 2012-2022 in dynamics, and the analysis of the contextual-time block of bibliometric analysis. As a result, the grouping of important determinants of the analysis of financial crime trends in different periods of time is clearly depicted (Figure 2), using different saturation of colours from purple to yellow, that is, from early publications to modern ones.

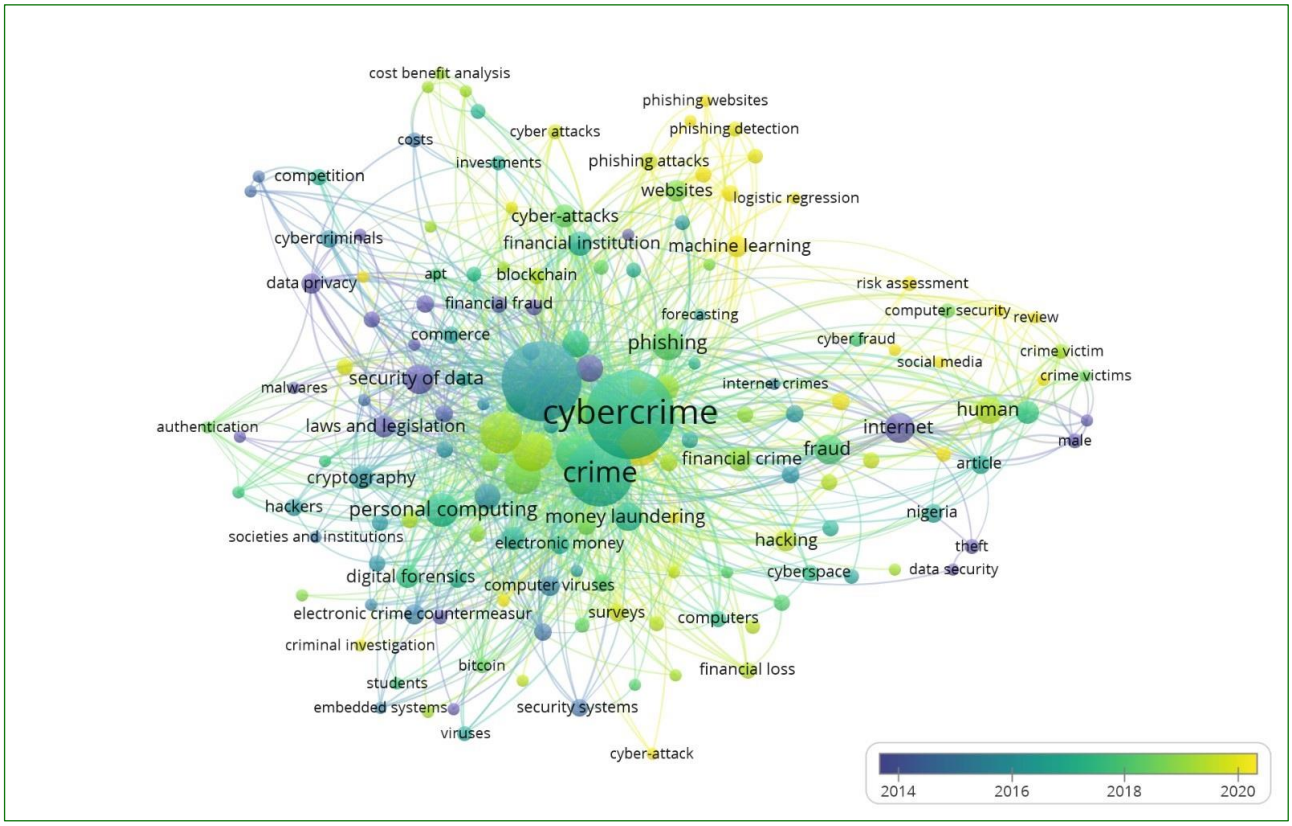

Figure 2. Visualization map of the contextual-temporal dimension of scientific assets in the editions of the Scopus database of concepts "financial crimes, cybercrime" for the period 2012-2022 in dynamics, using the VOSViewerv.1.6.15 software toolkit. *(Sources: developed/compiled/systematized by the authors based on the Scopus database using the VOSViewerv.1.6.15 software toolkit (Dotsenko, 2022)*

Thus, according to the analysis of the contextual-temporal block of scientific publications of the Scopus database of the categories "financial crimes, cybercrime" for the period 2012-2022 in dynamics, three main stages in the directions of research are outlined. In particular, from 2012 to 2014, the theoretical, regulatory, and legislative foundations of the possibility of conducting financial crimes on the Internet and their detection were studied. In the framework of 2015-2019, scientific interests were focused on the research of digital technologies, the storage of large-scale information, the use of extensive networks, numerous sites, the introduction of online services, the circulation of crypto-money, which also contributed to the spread of cyber fraud and the growth of the capabilities of cybercriminals. In the last years of 2020-2022, the vectors of modern researchers are increasingly directed toward machine learning, risk assessment, modeling, forecasting, and algorithmization of financial processes.

Based on the analysis of current trends in financial crime, we note that modern research areas on financial crimes envisage several research vectors.

An extremely important and meaningful area is the study of the sources and instruments of financial crimes, the definition of their main characteristics and features, the identification of typical situations and patterns of violations that are constantly changing in response to the situation in the financial market, taking into account the actions of the criminal world. First, we will highlight the exponentially growing number of devices with confidential financial data connected to the Internet, the expansion of cyberspace (the consequence of which is online attacks on the software and hardware of servers, network devices, single end users, using malware-viruses, trojans, spyware, in order to steal confidential information, checks by fraudsters of the level of protection of the object, gaining control over the computer equipment of the attack object; infection of the USB drive with the subsequent transfer of the infected device to other devices; Internet of Things botnets – a technology that allows establishing remote connections between smart devices through the Internet or

DOI: 10.55643/fcaptp.5.46.2022.3897

a similar network; a phishing threat to financial payments through fake sites causes fraudulent operations, breach of personal and corporate data, distribution of dangerous software; distribution of spam through extensive social media platforms; the butterfly effect software – a fraudulent program distributed by e-mail; data breach, indirect attack vulnerability, due to security flaws in web infrastructure, web applications, web downloads; gaps in the practical skills of cybersecurity workers, lack of cybersecurity specialists; issues with clouds of information resources – due to ubiquitous access to the network, pooling of resources for sharing, control and management of data by cloud service providers, the risk of cyber-attacks on these resources increases).

The modern sources and tools of financial crimes include the following: the use of the latest technologies by fraudsters – biometrics, artificial intelligence (fraudsters use such systems to sequentially scan the selected system and then attack it); inconsistent proliferation of the latest 5G technology (with its increased bandwidth, it contributes to an extremely rapid growth in the volume of devices and data, which does not correspond to the available control and security capabilities); excessive use of smart devices (the number of smart devices such as smartphones, smart TVs, smart watches, smart speakers, etc.) with the function of access via Bluetooth, Wi-Fi, mobile streams, does not meet the existing possibilities to ensure their safe use); distribution of cyber insurance (the disadvantages of this option are increasing in terms of targeting cyber fraudsters specifically at insured objects as they can potentially provide an opportunity for attackers to receive large amounts of money); cryptocurrency fraud: features of smart contracts in online services based on blockchain technology – cryptocurrency and Bitcoin, Ethereum (features and disadvantages of smart contracts are investigated: system security; user trust; own programming language; "hard forks"; rigid rules defined by the organization; high cost of training; lack of standardized interfaces; complex system for users; limited trading volumes due to increased transaction volumes and longer confirmation times; unresolved issues of implementation in terms of accessibility and use); financing the proliferation of weapons of mass destruction (purchase of dual-use goods; the use of free trade zones and transit centers for illegal transactions; use of schemes with front organizations; use of official financial institutions for illegal transactions).

Second, after identifying how financial fraud can be carried out, counteraction to financial crimes is developed by determining tactical measures using the following tools:

- providing supervision, detection, and prevention of risky and fraudulent transactions (continuous supervision of online transactions, including blockchain; priority of detection and prevention of illegal financial transactions at early stages based on information from risky sources; identification of shell organizations in financial schemes using a dynamic social network; use of the software package "Certified Threat Intelligence Analyst" – an analytical software that includes planning, analytics, threat reporting, training in the identification and threat control skills, and other features);
- the use of advanced latest tools of the IT industry (advanced machine learning, using built-in graphs to detect illegal activity; building models for assessing and forecasting illegal financial flows; the use of artificial intelligence technologies in the corporate financial risk management system, taking into account certain shortcomings of such technologies (insufficient interpretation for the implementation of due diligence); application of the group SHAP method in banking institutions to monitor customers (assessment of various indicators of the organization); practical application of knowledge engineering technology, as well as an ontology for crime investigation, which involves data generation, analysis, integration into the financial security system, identification of interrelations and trends in the actions of financial criminals, forecasting based on the use of semantic thinking tools and visualization of processes and knowledge)
- compliance with the regulations of the European Union on money laundering in terms of imposing restrictions on the use of tax havens (closing branches and offices of non-transparent financial institutions;
- development of innovative cyber defense systems with more efficient algorithms, protocols, and tools (protecting the network, using firewalls, antivirus software; online solutions for cyber security, managing cyber defense vulnerabilities when appropriate personnel is insufficient, cloud data security); use of flexible cybersecurity automation processes with integration; secure web framework with online vulnerability management; use of centralized marketplaces on smart devices – App Store, Play Market).

Third, special attention is paid to modelling financial crime. The following models may have practical applications:

- model of the topology and geometry of suspicious activity - involves the assessment of the mechanism of money laundering through financial networks; analysis of the topological structure of suspicious money laundering groups; the use of topological and geometric tools to identify the most relevant groups of subjects, agents in the network that carry out dubious and suspicious interactions related to money laundering. The methodology provides for the following stages: data collection; data analysis by applying network metrics (Total Nodes, Total Edges, Intermediar-

ies, Offshore Entities, Officers, Average Node Degree, Average Shortest Path Length, Assortativity, Connected Components, Detected Communities) to determine the degree of use of the node; determine the members of groups and the role of groups in the structure of illegal money laundering operations;

definition of the topological structure (using topology tools; network aspects related to links, description of the links between network nodes, which causes the distribution of paths and voids; the Euler characteristic is determined (Formula 1) – the topological invariant of the space characteristic encoding global network topological data [16]:

$$X(Y) = \sum_{n=0}^{N} -1^n |C_n| \quad (1)$$

Where X(Y) is a Euler characteristic, a finite set of all possible simplexes; Y-set, edge, set of linked nodes and vertices, C_n *– a subset of all n-simplexes C(E).*

definition of a geometric structure (using discrete geometry tools; aspects related to size, network distance, curvature; definition of a discrete quantity – Forman–Ricci curve (Formula 2) – a tool for describing network geometry [16]:

$$FR\,(e) = 2 - |\{e' \epsilon E : e' \| e\}| = 4 - \sum_{v \sim e} d(v) \quad (2)$$

Where - $FR\,(e)$ *- Forman-Ricci curvature,* $e' \epsilon E$ *- number of vertices,* $\|$ *- concurrency,* $\sim$ *- incidence.*

This complex model culminates in a visual representation of suspicious money laundering groups on the network.

- network analysis model – determining the effect of anti-money laundering policies by analyzing an empirical network. The conceptual framework and network analysis model provides for the following: defining measures of centrality to reveal the inner workings of the network, as well as understanding the structural importance of certain nodes (degree centrality, mediation centrality, proximity centrality); establishing structural measures to explain the strategic reasons for establishing certain links (assortativity index, transitivity index, constraints and structural holes); taking into account the cluster level, the established hypotheses and the specification of the model are tested (the first hypothesis is that the specialization of money laundering causes one of three specific results; the second hypothesis is that the specialization of persons engaged in money laundering prompts specialists in money laundering to take one of three specific actions); implementation of statistical econometric analysis based on clusters and nodes for various variables to test the hypotheses suggested in the paper (two options are tested:

  Formula 3 describes how each indicator varies depending on the criminal group over time [15]:

$$x_{it} = A_0 + A_1\varphi_{it} + A_2 c_{it} + A_3 a_t + \alpha_i + \theta_{it} \quad (3)$$

Where x_{it} *- dependent variable;* A_0 *– coefficient provides segment, intercept;* A_1 *,* A_2 *– coefficients indicating the difference between criminal clusters with and without money laundering;* A_3 *– impact factor for all clusters;*

Formula 4 represents a dependent variable from Formula 3, but with the addition of a term [15]:

$$x_{it\tau} = A_0 + A_1\varphi_i + A_2 c_i + A_3 a_t + \tau_1\varphi_i\alpha_t + \tau_2 c_i\alpha_t + \vartheta_{it} \quad (4)$$

Where τ_1 *– coefficient of the money laundering cluster;* τ_2 *- coefficient of other criminal clusters;* a_t *– a dummy variable indicating a term or period);*

analysis of social networks (calculation of centralities, clustering); temporary network clustering (to determine the interconnections between groups of nodes, dynamics of related clusters); visualization of results. The results of this model allow getting an idea of the degree of interrelations, cooperation, and competition between criminal structures, fraudsters, and persons engaged in money laundering in network structures.

- modeling the identification of shell companies in financial institutions using a dynamic social network. Identifying shell companies involves the use of a methodology with the group and independent comparison in dynamic social networks. The methodology of the model includes: social networks and applications – the interaction of people at the national and international levels (a social network is a set of many edges and links between them, defined by Formula 5 [46]:

$$CC = (B, R) \quad (5)$$

DOI: 10.55643/fcaptp.5.46.2022.3897

Where CC - social network; $B = \{b_1 b_2, \ldots, b_n\}$ – finite non-empty set of vertices; $R = \{r_1 r_2, \ldots, r_m\}$ – final non-empty set of edges; n – number of vertices; m – number of edges);

the concept of a dynamic social network (a social network with changes over a certain period, defined by Formula 6 [46]:

$$CC_t = \{(B_t, R_t)\}_t^T \quad (6)$$

Where CC - social network; $B_t = \{b_{t,1} b_{t,2}, \ldots, b_{t,n}\}$ – finite non-empty set of vertices; $R_t = \{r_{t,1} r_{t,2}, \ldots, r_{t,m}\}$ – final non-empty set of edges; $t = 1,2, \ldots, T$) – time period);

definition of a set of attributes of legal entities and individuals; formation of a database, variables (variable for tracking false accounts; economic activity; politically exposed persons; transactions with the government; address matching; virtual institutions; joint shareholders; common legal representatives; shared addresses; matching transactions with business assets; the logic of financial activity; matching escrow resources, age of shareholders; period of employment in the institution; creation of networks and intensives); programming an expert system (assigning risk metrics, calculating the connection intensity to detect suspicious activity, setting up a self-comparison process based on the dynamics of past social networks, calculating the optimal risk threshold, identification of suspicious cases); construction of a methodology flow; formation of an automated calculation algorithm; visualization of research results.

- visualization modeling of financial fraud detection based on the ATOVis tool [33] – a visualization tool that analyzes and detects suspicious activity quickly. The model includes stages: abstraction of the task to identify the scheme of financial crime (subtasks: detection of illegal transactions, determination of successive changes in transaction attributes, analysis of transaction models for typical and atypical, detection of reuse of specific attributes, analysis of attribute values, detailed verification of the operation to determine the level of risk; taxonomy of visual tasks – categorization of transactions, comparison and ranking of transactions, distinction and underlining of transactions, correlation, identification; task design – tracking transactional behavior, timing of transactions, generalization of statistical data and information about transactions; building two ATOVis visualization models (visualization models are based on attribute changes and transaction frequency; ATOVis is represented by a functional application based on Java and Processing; includes reflection of financial agreement representation, financial behavior clustering, visual display of transaction attributes connectivity, implementation of cluster interaction methods; formation of a multi-scale timeline for viewing data to implement the ability to move through all transactions (allows quickly analyzing the frequency of transactions, as well as their distribution, highlighting the period under study; consists of two parts – an overview (an overview of all transactions) and a detailed one (image of the temporal distribution of transactions); the scale is based on an adaptive mechanism).

DISCUSSION

Revolutionary innovations in technology result in the latest threats to the financial sector. And a clear understanding of modern threats in different countries of the world in the financial sphere, sources and tools of financial fraud, significantly affects the success of tools for combating financial crimes [6, 11, 21]. Thus, a bibliometric analysis of scientific publications dedicated to the study of the latest trends in financial crime, analysis of key scientific categories in the researched question "health care system, medical services, behavioral aspect, social aspect", in contrast to such methods and techniques of the theory of knowledge as analysis, synthesis, induction, deduction, logical method, comparative-historical methods, the establishment of cause-and-effect relationships of the development of processes, provided the possibility of conducting content-contextual, contextual-but-temporal thanks to the services of the Scopus information platform and the VOSViewerv.1.6.15 toolkit, which is also confirmed by the effectiveness of using this technique in the works of other modern scientists [10, 23]. At the same time, in the conditions of intensification of technical and technical progress not only for legal financial activities but also for the capture of similar opportunities by fraudsters, the author's proposals also consist in the need for the complex use of various processes of financial crime models for the future safe functioning of the financial sector. The relevance of modeling aspects related to financial crime is becoming increasingly widespread in the scientific world community [3, 29, 33, 46]. Thus, for the effective development of the financial system in the countries of the world, it is advisable to regularly review the existing strategic approaches and theories of financial security in order to identify inefficient, irrelevant components, to implement a timely search for the newest basis, which would innovatively, comprehensively and effectively meet the needs of today's financial world.

CONCLUSIONS

Thus, usually, the center of financial fraud deals with the turnover of illegal money from money laundering, criminal transactions, and illegal financial transactions. In turn, the bibliometric analysis of scientific publications dedicated to the study of the latest trends in financial crime made it possible to meaningfully systematize and formalize theoretical achievements in a certain direction, to implement a substantive-contextual, evolutionary-dynamic study of the key categories of "financial crimes, cybercrime". It is established that financial crime has been studied for a long time, but aspects of cybercrime are relatively new and will require in-depth consideration. Analyzing the research vectors of modern trends in financial crime, we note that each of the potential sources and tools of financial fraud with their negative, harmful aspects should be identified, considered in depth, and studied: the exponentially growing number of devices with confidential financial data connected to the Internet, the expansion of cyberspace; the use of the latest technologies by fraudsters – biometrics, artificial intelligence; the controversial spread of the latest 5G technology; excessive use of smart devices; distribution of cyber insurance; crypto-currency fraud – peculiarities of smart contracts in online services based on blockchain technology – cryptocurrency and Bitcoin, Ethereum; financing of the proliferation of weapons of mass destruction must be identified, considered and studied in depth. Appropriate tools for countering financial crime should be developed: ensuring supervision, detection, and prevention of risky and fraudulent transactions; application of advanced latest IT industry tools; compliance with the European Union regulations on money laundering; development of innovative cyber security systems with more efficient algorithms, protocols, and tools. Particular attention should be paid to modeling financial crime: a model of topology and geometry of suspicious activity; a network analysis model; modeling the detection of shell companies in financial institutions through a dynamic social network; modeling the visualization of financial fraud detection based on the use of the ATOVis tool. Thus, these vectors can be practically applied by financial organizations, institutions, and business entities for the future safe functioning of the financial sector but taking into account the need for constant development of IT support for financial transactions as a response to the rapidly changing needs of our time.

ADDITIONAL INFORMATION

FUNDING

This research was funded by a grant from the Ministry of Education and Science of Ukraine (No. s/r 0121U100467, 0122U000783); 0121U109559 National Security Through the Convergence of Financial Monitoring and Cybersecurity Systems: Intelligent Modeling of Financial Market Regulation Mechanisms.

This article is an output of the project of the Scientific Grant Agency of the Ministry of Culture of the Slovak Republic and Slovak Academy of Sciences (VEGA) no. 1/0517/20 (2020-2022) "Virtual Cryptochains as a Relevant Tool to Eliminate Economic Crime."

This work was supported by the Ministry of Education and Science of Ukraine (0122U000774 «Digitalization and transparency of public, corporate and personal finance: the impact on innovation development and national security»).

REFERENCES

1. Agbor, A. A. (2022). A delineation of the impact of illicit financial flows on the right to development: Details from Cameroon's special criminal court. *Journal of Financial Crime*, DOI: https://doi.org/10.1108/JFC-03-2022-0071.
2. Agnihotri, A., & Gupta, S. (2019). Relationship of Corporate Governance and Efficiency of Selected Public and Private Sector Banks in India. *Business Ethics and Leadership, 3*(1), 109-117. http://doi.org/10.21272/bel.3(1).
3. Alikariev, O.F.U., & Poliakh, S. (2018). Index of protection of the interests of consumers of the financial services market. *Business Ethics and Leadership, 2*(1), 78-95. DOI: https://doi.org/10.21272/bel.2(1).78-95.2018.
4. Al-Khonain, S., & Al-Adeem, K. (2020). Corporate Governance and Financial Reporting Quality: Preliminary Evidence from Saudi Arabia. Financial Markets, Institutions and Risks, 4(1), 109-116. http://doi.org/10.21272/fmir.4(1).109-116.2020.
5. Antonyuk, N., Plikus, I., & Jammal, M. (2021). Human Capital Quality Assurance under the Conditions of Digital Business Transformation and COVID-19 Impact. *Health Economics and Management Review, 2*(3), 39-47. https://doi.org/10.21272/hem.2021.3-04.

DOI: 10.55643/fcaptp.5.46.2022.3897

6. Baltgailis, J., & Simakhova, A. (2022). The Technological Innovations of Fintech Companies to Ensure the Stability of the Financial System in Pandemic Times. *Marketing and Management of Innovations*, 2, 55-65. https://doi.org/10.21272/mmi.2022.2-05.

7. Berzin, Pavlo , Shyshkina, Olena , Kuzmenko, Olha , & Yarovenko, Hanna (2018). INNOVATIONS IN THE RISK MANAGEMENT OF THE BUSINESS ACTIVITY OF ECONOMIC AGENTS. *MARKETING AND MANAGEMENT OF INNOVATIONS*, 4, 221-233. https://www.webofscience.com/wos/woscc/full-record/WOS:000459816600020.

8. Boronos, V., Zakharkin, O., Zakharkina, L., & Bilous, Y. (2020). The impact of the covid-19 pandemic on business activities in Ukraine. *Health Economics and Management Review*, 1(1), 76-83. https://doi.org/10.21272/hem.2020.1-07.

9. Bouchetara, M., Nassour, A., & Eyih, S. (2020). Macroprudential policy and financial stability, role and tools. *Financial Markets, Institutions and Risks*, 4(4), 45-54. https://doi.org/10.21272/fmir.4(4).45-54.2020.

10. Bozhenko, V., & Kuzmenko, O. (2021). LINKAGES BETWEEN SHADOW ECONOMY AND CORRUPTION: A BIBLIOMETRIC ANALYSIS. *FINANCIAL AND CREDIT ACTIVITY-PROBLEMS OF THEORY AND PRACTICE*, 39(4), 176-185. https://www.webofscience.com/wos/woscc/full-record/WOS:000724738800002.

11. Bulut, H., & Kacar, F. (2022). Prevention of cyberattacks on SCADA systems used in the financial sector. *Electrica, 22*(2), 132-142. DOI: https://doi.org/10.54614/electrica.2022.22004.

12. Buriak, A., Lyeonov, S., & Vasylieva, T. (2015). Systematically Important Domestic Banks: An Indicator-Based Measurement Approach for the Ukrainian Banking System. Prague Economic Papers, 24(6), 715-728. DOI: https://doi.org/10.18267/j.pep.531.

13. Djamila, T.A., & Abdelatif, M. (2022). The Impact of Setting up a Cloud Computing Solution on Small and Medium Organization's Management: A Qualitative Study. *Business Ethics and Leadership, 6*(1), 33-38. https://doi.org/10.21272/bel.6(1).33-38.2022.

14. Formankova, S., Trenz, O., Faldik, O., Kolomaznik, J., & Vanek, P. (2018). The future of investing – sustainable and responsible investing. Marketing and Management of Innovations, 2, 94-102. https://doi.org/10.21272/mmi.2018.2-08.

15. Gerbrands, P., Unger, B., Getzner, M., & Ferwerda, J. (2022). The effect of anti-money laundering policies: An empirical network analysis. EPJ Data Science, 11(1). https://doi.org/10.1140/epjds/s13688-022-00328-8.

16. Granados, O. M., & Vargas, A. (2022). The geometry of suspicious money laundering activities in financial networks. EPJ Data Science, 11(1). https://doi.org/10.1140/epjds/s13688-022-00318-w.

17. Gupta, A., & Mishra, M. (2022). Ethical Concerns While Using Artificial Intelligence in Recruitment of Employees. *Business Ethics and Leadership, 6*(2), 6-11. https://doi.org/10.21272/bel.6(2).6-11.2022.

18. Jenjira Phomkamin, Chalita Pumpuang, Pattarawan Potijak, Supaporn Sangngam, Issariya Ketprasit, & Bahaudin G. Mujtaba. (2021). Engagement Strategies for E-commerce Businesses in the Modern Online World. *SocioEconomic Challenges, 5*(4), 24-34. https://doi.org/10.21272/sec.5(4).24-34.2021.

19. Juarez-Garcia, M.I., (2020). Personal Corruption & Corrupting Laws: Montesquieu's Twofold Theory of Corruption. Business Ethics and Leadership, 4(4), 76-84. http://doi.org/10.21272/bel.4(4).76-83.2020.

20. Kaya, H.D., & Engkuchik, E.N.S. (2021). The Perception of Corruption Among Retailers in Central Asia and Eastern Europe During and After the 2008 Crisis. *SocioEconomic Challenges, 5*(2), 70-80. https://doi.org/10.21272/sec.5(2).70-80.2021.

21. Klimczak, K. M., Sison, A. J. G., Prats, M., & Torres, M. B. (2022). How to deter financial misconduct if crime pays? *Journal of Business Ethics, 179*(1), 205-222. DOI: https://doi.org/10.1007/s10551-021-04817-0.

22. Kuzmenko, O. V., & Koibichuk, V. V. (2018). ECONOMETRIC MODELING OF THE INFLUENCE OF RELEVANT INDICATORS OF GENDER POLICY ON THE EFFICIENCY OF A BANKING SYSTEM. *CYBERNETICS AND SYSTEMS ANALYSIS*, 54(5), 687-695. https://www.webofscience.com/wos/woscc/full-record/WOS:000446410700001.

23. Kuzmenko, O. V., Kubálek, J., Bozhenko, V. V., Kushneryov, O. S., & Vida, I. (2021). An approach to managing innovation to protect financial sector against cybercrime. [Podejście do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością] *Polish Journal of Management Studies*, 24(2), 276-291. DOI: https://doi.org/10.17512/pjms.2021.24.2.17.

24. Kuzmenko, O., Lieonov, S., & Kashcha, M. (2020). FINANCIAL, ECONOMIC, ENVIRONMENTAL AND SOCIAL DETERMINANTS FOR UKRAINIAN REGIONS

DIFFERENTIATION BY THE VULNERABILITY LEVEL TO COVID-19. *FINANCIAL AND CREDIT ACTIVITY-PROBLEMS OF THEORY AND PRACTICE, 34*(3), 270-282. https://www.webofscience.com/wos/woscc/full-record/WOS:000588420200027.

25. Lyeonov, Serhiy, Kuzmenko, Olha, Yarovenko, Hanna, & Dotsenko, Tatiana (2019). THE INNOVATIVE APPROACH TO INCREASING CYBERSECURITY OF TRANSACTIONS THROUGH COUNTERACTION TO MONEY LAUNDERING. *MARKETING AND MANAGEMENT OF INNOVATIONS*, 3, 308-326. https://www.webofscience.com/wos/woscc/full-record/WOS:000496556500005.
26. Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. Paper presented at the *CEUR Workshop Proceedings, 2422*, 297-307. Retrieved from www.scopus.com
27. Levchenko, V., Boyko, A., Savchenko, T., Bozhenko, V., Humenna, Yu. & Pilin, R. (2019). State regulation of the economic security by applying the innovative approach to its assessment. *Marketing and Management of Innovations*, 4, 364-372. https://doi.org/10.21272/mmi.2019.4-28.
28. Li, M. (2022). A survey on ethereum illicit detection DOI: https://doi.org/10.1007/978-3-031-06791-4_18 Retrieved from www.scopus.com.
29. Lin, K., & Gao, Y. (2022). Model interpretability of financial fraud detection by group SHAP [formula presented]. Expert Systems with Applications, 210. DOI: https://doi.org/10.1016/j.eswa.2022.118354.
30. Lopez, B.S., Caetano, I.M.S., & Alcaide, A.V. (2022). Innovation and Social Networks for Creating Social Value. *SocioEconomic Challenges, 6*(2), 94-105. https://doi.org/10.21272/sec.6(2).94-105.2022.
31. Louis, R. (2017). A new economic order for global prosperity. SocioEconomic Challenges, 1(2), 52-59. http://doi.org/10.21272/sec.1(2).52-59.2017.
32. Lyulyov, O., Paliienko, M., Prasol, L., Vasylieva, T., Kubatko, O., & Kubatko, V. (2021). Determinants of shadow economy in transition countries: Economic and environmental aspects. *International Journal of Global Energy Issues, 43*(2-3), 166-182. Retrieved from http://www.inderscience.com/ijgei.
33. Maçãs, C., Polisciuc, E., & Machado, P. (2022). ATOVis – A visualisation tool for the detection of financial fraud. Information Visualization, 21(4), 371-392. DOI: https://doi.org/10.1177/14738716221098074
34. Mahi-Al-rashid, A., Hossain, F., Anwar, A., & Azam, S. (2022). False data injection attack detection in smart grid using energy consumption forecasting. *Energies, 15*(13) DOI: https://doi.org/10.3390/en15134877.
35. Matvieieva, Yu., & Hamida, H.B. (2022). Modelling and Forecasting Energy Efficiency Impact on the Human Health. *Health Economics and Management Review, 3*(2), 78-85. https://doi.org/10.21272/hem.2022.2-09
36. Meresa, M. (2019). The Effect of Strategic Management Practices on the institutional Performance; the case of Dedebit credit and saving institution in Eastern Tigray. *SocioEconomic Challenges, 3*(3), 80-97. http://doi.org/10.21272/sec.3(3).80-97.2019.
37. Morsher, Ch., Horsch A., & Stephan J. (2017). Credit Information Sharing and Its Link to Financial Inclusion and Financial Intermediation. *Financial Markets, Institutions and Risks, 1*(3), 22-33. DOI: https://doi.org/10.21272/fmir.1(3).22-33.2017.
38. Muradov, İ. (2022). Problems Of E-Governance İn Government Agencies and Their Solutions. *SocioEconomic Challenges, 6*(1), 79-86. https://doi.org/10.21272/sec.6(1).79-86.2022.
39. Müller, W., Mühlenberg, D., Pallmer, D., Zeltmann, U., Ellmauer, C., & Demestichas, K. (2022). Knowledge engineering and ontology for crime investigation. DOI: https://doi.org/10.1007/978-3-031-08333-4_39.
40. Naseer, M.M., Guo, Y., & Zhu, X. (2022). Stock Performance, Sector's Nature and Macroeconomic Environment. *Financial Markets, Institutions and Risks, 6*(1), 13-26. https://doi.org/10.21272/fmir.6(1).13-26.2022.
41. Oliinyk, O. S., Shestopalov, R. M., Zarosylo, V. O., Stankovic, M. I., & Golubitsky, S. G. (2022). Economic security through criminal policies: A comparative study of western and european approaches. [La seguridad económica a través de las políticas criminales: estudio comparativo de los enfoques occidental y europeo] Revista Cientifica General Jose Maria Cordova, 20(38), 265-285. DOI: https://doi.org/10.21830/19006586.899.
42. Oloveze, A.O, Ugwu, P.A., Okonkwo, R.V.O., Okeke, V.C., Chukwuoyims, K., & Ahaiwe, E.O. (2022). Factors motivating end-users' behavioural intention to recommend m-health innovation: multi-group analysis. *Health Economics and Management Review, 3*(3), 17-31. https://doi.org/10.21272/hem.2022.3-02.

DOI: 10.55643/fcaptp.5.46.2022.3897

43. Pandey, A. B., Tripathi, A., & Vashist, P. C. (2022). A survey of cyber security trends, emerging technologies and threats. DOI: https://doi.org/10.1007/978-981-16-8012-0_2.

44. Quintel, T. (2022). Data protection rules applicable to financial intelligence units: Still no clarity in sight. ERA Forum, 23(1), 53-74. DOI: https://doi.org/10.1007/s12027-021-00697-z.

45. Rizk, S. (2022). Efficiency in the MENA banking industry, the stochastic frontier approach (SFA). *Financial Markets, Institutions and Risks, 6*(2), 56-59. https://doi.org/10.21272/fmir.6(2).56-59.2022

46. Rocha-Salazar, J.-d.-J., Segovia-Vargas, M.-J., & Camacho-Miñano, M.-d.-M. (2022). Detection of shell companies in financial institutions using dynamic social network. Expert Systems with Applications, 207 DOI: https://doi.org/10.1016/j.eswa.2022.117981.

47. Rose, K. J. (2022). EU money laundering regulation limit the use of tax havens. *Journal of Financial Crime, 29*(1), 233-245. DOI: https://doi.org/10.1108/JFC-12-2020-0253.

48. Rubanov, P., Lyeonov, S., Bilan, Y., & Lyulyov, O. (2019, November). The Fintech sector as a driver of private entrepreneurship development in time of industry 4.0. In Conference proceedings: The Impact of Industry (Vol. 4, pp. 319-328).

49. Rubanov, P., Vasylieva, T., Lyeonov, S., & Pokhylko, S. (2019). Cluster analysis of development of alternative finance models depending on the regional affiliation of countries. *Business and Economic Horizons, 15*(1), 90-106. http://dx.doi.org/10.15208/beh.2019.6.

50. Sallaberry, J. D., & Flach, L. (2022). Analysis of whistleblower beliefs in latin america. [Análise das crenças whistleblower na América Latina; Análisis de las creencias whistleblower en América Latina] Revista Criminalidad, 64(1), 133-153. DOI: https://doi.org/10.47741/17943108.336.

51. Samoilikova, A., & Kunev, R. (2020). The impact of health care financing on the economic growth: EU countries analysis. *Health Economics and Management Review, 1*(2), 24-32. https://doi.org/10.21272/hem.2020.2-03.

52. Serpeninova, Yu., Makarenko, I., Plastun, A., Babko, A., & Gasimova, G. (2020). Mapping of the responsible investment's instruments in sdg 3 'good health and well-being' financing: EU and US experience. *Health Economics and Management Review, 1*(1), 106-115. https://doi.org/10.21272/hem.2020.1-10.

53. Singh, V., & Sharma, S. K. (2022). Application of blockchain technology in shaping the future of food industry based on transparency and consumer trust. *Journal of Food Science and Technology*. DOI: https://doi.org/10.1007/s13197-022-05360-0.

54. Skrynnyk, O. (2021). Analysis of Corporate Investment Behaviour in Digital Technologies for Organisational Development Purposes. *Financial Markets, Institutions and Risks, 5*(3), 79-86. https://doi.org/10.21272/fmir.5(3).79-86.2021.

55. Stavrova, E. (2021). Banks' Digital Challenges. *Business Ethics and Leadership, 5*(3), 87-96. https://doi.org/10.21272/bel.5(3).87-96.2021.

56. Taghieva, T., & Tiutiunyk, I. (2022). Innovative, Economic and Marketing Determinants of Financial Security and Sustainability of Business. *Marketing and Management of Innovations*, 1, 176-185. https://doi.org/10.21272/mmi.2022.1-13.

57. Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. Crime Science, 11(1). DOI: https://doi.org/10.1186/s40163-021-00163-8.

58. Wang, S., Zhu, X., & Zhang, B. (2022). A new financial crime: Proliferation financing and China's countermeasures. Security Journal. DOI: https://doi.org/10.1057/s41284-022-00340-7.

59. Yarovenko, H., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Methodology for assessing the risk associated with information and knowledge loss management. *Journal of Business Economics and Management, 22*(2), 369-387. https://doi.org/10.3846/jbem.2021.13925.

60. Yeh, S. S. (2022). New OSCE recommendations to combat corruption, money laundering, and the financing of terrorism. Laws, 11(2). DOI: https://doi.org/10.3390/laws11020023.

61. Zarutska, E., Pavlova, T., & Sinyuk, A. (2018). Structural-functional analysis as innovation in public governance (case of banking supervision*). Marketing and Management of Innovations*, 4, 349-360. https://doi.org/10.21272/mmi.2018.4-30.

Zatonatska, T., Hubska, M., & Shpyrko, V. (2022). Marketing Strategies in the Banking Services Sector with the Help of Data Science. *Marketing and Management of Innovations*, 2, 121-127. https://doi.org/10.21272/mmi.2022.2-11.

Сігетова К., Узікова Л., Доценко Т., Бойко А.

ОСТАННІ ТЕНДЕНЦІЇ ФІНАНСОВОЇ ЗЛОЧИННОСТІ СВІТУ

У статті підкреслено, що цифровізація сучасного світу, розвиток інформаційних технологій, поширення Internet, комп'ютерні мережі, використання кіберпростору полегшили повсякденне життя суспільства, але паралельно з цим спричинили загрозу безпеці та конфіденційності інформації, особистих даних, фінансової системи. Наголошено, що фінансове шахрайство стає все більш серйозною глобальною макропроблемою, оскільки фінансова екосистема також використовується кримінальним світом для відмивання нелегальних коштів та проведення незаконних фінансових транзакцій. Основна мета дослідження – визначення останніх тенденцій фінансової злочинності світу. Як методичний інструментарієй дослідження використано теоретичні методи дослідження – групування, абстрагування; емпіричні методи дослідження – спостереження, опис; ресурсну базу інформаційної платформи, бібліометричний аналіз, моделювання. Об'єкти дослідження – такі наукові категорії: регулятивно-правові та нормативно-законодавчі аспекти фінансових злочинів, онлайн-злочини та кіберзлочини; методики та системи регулювання, контролю, попередження, протидії, боротьби з фінансовою злочинністю; моделювання процесів фінансової злочинності. Проаналізовано праці світових науковців щодо зміщення центру інтересів сучасних науковців фінансового ринку на дослідження особливостей фінансової злочинності. Актуальність визначення останніх тенденцій фінансової злочинності полягає в тому, що дослідження тенденцій фінансової злочинності допоможе покращити поінформованість про фінансові шахрайства, створити спільні бази даних, утворити коаліції, визначити ефективні та дієві способи, що сприятимуть підвищенню спроможності боротьби з фінансовими злочинами на більш ефективному національному та світовому рівні. На початковому етапі роботи проведено бібліометричний аналіз наукових публікацій, присвячених дослідженню останніх тенденцій фінансової злочинності. У результаті систематизовано літературні напрацювання до вивчення зазначеного питання; сформовано мапу взаємозв'язків між ключовими термінами та іншими науковими поняттями; проведено змістовно-контекстуальний та міжкластерний аналіз отриманих блоків бібліометричного аналізу; побудовано мапу взаємозв'язків досліджуваних ключових понять із іншими науковими категоріями в динаміці та проаналізовано контекстуально-часовий блок. Дослідження складається з трьох частин, що передбачають визначення кількох векторів роботи . Як результат дослідження – виділено потенційні джерела та інструменти фінансових шахрайств із їхніми негативними, шкідливими аспектами для ідентифікації, поглибленого розгляду та вивчення; визначено відповідні інструменти протидії фінансовим злочинам; описано практичні моделі для оцінки, аналізу, виявлення, порівняння, візуалізації особливостей фінансової злочинності. Висновок дослідження передбачає, що отримані результати можуть бути практично застосовані фінансовими організаціями, установами, суб'єктами господарювання для майбутнього безпечного функціонування фінансового сектора, але з урахуванням потреби постійного розвитку інформаційно-технологічного забезпечення фінансових операцій, як відповідь на запити швидко змінюваних потреб сучасності.

Ключові слова: фінансові злочини, кіберзлочини, відмивання коштів, ризикові фінансові операції, кіберзахист, моделювання фінансової злочинності

JEL Класифікація: K00, K22, G24

DOI: 10.55643/fcaptp.5.46.2022.3897