DOI: https://doi.org/10.32782/2308-1988/2023-47-7
UDC 004.056.5;351.77;343.72

Tetiana Dotsenko
Sumy State University; Technical University of Berlin, Germany
Mykhailo Kuzmenko
Academic and Research Institute of Business, Economics and Management
Sumy State University

Доценко Тетяна Віталіївна
доктор філософії, асистент кафедри економічної кібернетики,
Сумський державний університет;
Технічний університет Берліну, Німеччина
ORCID: https://orcid.org/0000-0001-5713-2205
Кузьменко Михайло Володимирович
аспірант кафедри менеджменту,
Навчально-науковий інститут бізнесу, економіки та менеджменту
Сумського державного університету
ORCID: https://orcid.org/0009-0008-2049-5190

CYBER FRAUD AS A THREAT TO THE SUSTAINABLE DEVELOPMENT OF THE HEALTH CARE SYSTEM: A SYSTEMATIC BIBLIOMETRIC ANALYSIS[1]

КІБЕРШАХРАЙСТВО ЯК ЗАГРОЗА СТАЛОМУ РОЗВИТКУ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я: СИСТЕМНИЙ БІБЛІОМЕТРИЧНИЙ АНАЛІЗ

Summary. There is a growing wave of cyber fraud in the healthcare industry. Cases of breaches of confidentiality and security, leakage, theft and breach of medical confidential data, and fraudsters gaining access to machines and networks of medical institutions have become more frequent. The main purpose of the study is a retrospective and current systematic bibliometric analysis of scientific research in the field of cyber fraud as a threat to the sustainable development of the health care system based on Scopus, VOS Viewer, Statista. The relevance of solving this scientific problem lies in conducting not a traditional, but a comprehensive innovative systematic study of the industry, identifying priority dynamic, geographical and inter-sectoral links and directions, and problematic aspects. The research was carried out in the following logical sequence: determining the criteria for selecting publications on cyber fraud in the healthcare system; determining the dynamics of scientific articles in this area; analyzing the geographical distribution of research; studying the distribution of subject areas of the problem under study; forming and analyzing clusters of scientific articles on cyber fraud in the healthcare system by key terms; building an evolutionary and temporal map of the relationships of the studied categories with other scientific concepts in dynamics. Scopus platform, VOS Viewer software, Statista statistical database were used as analytical tools for the study. The study theoretically proves the existence of a close relationship between the health care system and cyber fraud. The results of the proposed model of a comprehensive systematic study of the healthcare industry will allow timely identification of priority areas and problematic aspects of the industry in terms of cybersecurity, will improve the protection of patients, patient data, hospital security management, strengthen the protection of medical devices, minimize the risks of cyber losses in the healthcare system, to organize sustainable development of the healthcare industry, to ensure good health of people.

Keywords: cyber fraud, cyber security, healthcare system, bibliometric analysis, cluster, good health of people, sustainable development.

[1] The article was written during a research stay at the Technical University of Berlin, Department of Health Care Management. The work was performed within the scope of the research topic "Data-Mining for countering cyber fraud and legalization of criminal proceeds in the conditions of digitalization of the financial sector of the economy of Ukraine", state registration number: 0121U100467; "Modeling the mechanisms of detinization and decorruption of the economy to ensure national security: the impact of the transformation of financial behavioral patterns", state registration number: 53.16.01-22/24.3П-01; the topic "National security through the convergence of financial monitoring systems and cyber security: intelligent modeling of financial market regulation mechanisms" state registration number: 0121U109559.

Анотація. У галузі охорони здоров'я зростає хвиля кібершахрайства. Основною метою проведеного дослідження є ретроспективний і поточний системний бібліометричний аналіз наукових досліджень за напрямком кібершахрайства як загроза сталому розвитку системи охорони здоров'я. Актуальність вирішення даної наукової проблеми полягає у проведенні не традиційного, а комплексного інноваційного систематичного дослідження галузі, виявленні пріоритетних виявлення динамічних, географічних і міжгалузевих зв'язків і напрямків, проблемних аспектів. Дослідження виконано в наступній логічній послідовності: визначення критеріїв відбору публікацій з тематики кібершахрайств у системі охорони здоров'я; визначення динаміки наукових статей із зазначеного напрямку; аналіз географічного розподілу досліджень; вивчення розподілу предметних областей досліджуваної проблеми; формування та аналіз кластерів наукових статей з кібершахрайств у системі охорони здоров'я за ключовими термінами; побудова еволюційно-часової мапи взаємозв'язків досліджуваних категорій з іншими науковими поняттями у динаміці; визначення та аналіз напрямків розподілу кібератак у галузі охорони здоров'я за векторами на основі відомостей. В якості аналітичних інструментів дослідження застосовано платформи Scopus, ПЗ VOS Viewer, статистична база даних Statista. У дослідженні теоретично доведено наявність тісного взаємозв'язку системи охорони здоров'я та кібершахрайств. Результати запропонованої моделі комплексного систематичного дослідження галузі охорони здоров'я, дозволять вчасно виявляти пріоритетні напрямки та проблемні аспекти галузі в аспекті кібербезпеки, дозволить покращити забезпечення захисту пацієнтів, даних пацієнтів, управління безпекою лікарень, посилити захист медичних пристроїв, мінімізувати ризики кібервтрат у системі охорони здоров'я, для організації сталого розвитку галузі охорони здоров'я, для забезпечення міцного здоров'я людей.

Ключові слова: кібершахрайство, кібербезпека, система охорони здоров'я, бібліометричний аналіз, кластер, міцне здоров'я людей, сталий розвиток.

Problem statement. There is a growing wave of cyber fraud in the healthcare industry. Cases of cyber fraud in the healthcare system have reached a level where they cannot be ignored. Thus, in 2022, the share of cybersecurity incidents in the healthcare sector amounted to 5.8% of all industries, as evidenced by the distribution of cyberattacks in world industries (Figure 1) [2].

Cybercriminals are using new, sophisticated, but insidious and dishonorable methods to cause healthcare fraud that are difficult for law enforcement to track and identify. Thus, in the healthcare sector, there have been more frequent cases of privacy and security breaches, leaks, theft and violations of medical, confidential data, fraudsters gaining access to machines and networks, phishing, and others [4]. This leads to disruptions in the processes of diagnosis, treatment, and life support of patients by medical professionals.

To counter such threats, the management of healthcare institutions and organizations, healthcare professionals, and healthcare risk managers need to effectively anticipate fraud schemes by taking proactive and preventive measures.

Therefore, in order to organize the sustainable development of the healthcare sector, to ensure good health of people, it is important to conduct comprehensive systematic research in this area on an ongoing basis, identify priority areas and problematic aspects, and, based on the results and experience of such research, improve the system of cybersecurity measures for comprehensive, effective counteraction to cyber fraud.

Analysis of recent research and publications. Analyzing the publications of the Scopus database in the direction of cyberfraud research in the healthcare system, we can conclude that this topic is quite new and not sufficiently studied, although there are certain theoretical and practical developments in this areas.

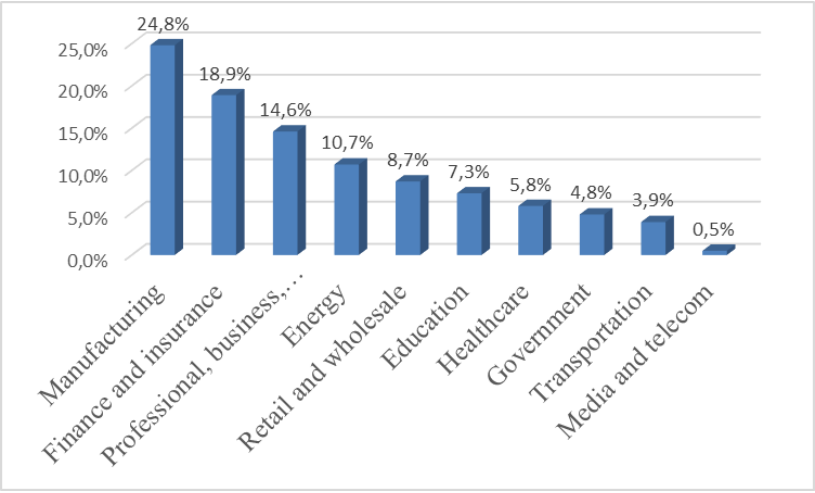

Figure 1 – Distribution of cyber attacks across worldwide industries in 2022

Source: systematized by the authors

Given the research of global scholars on cyber fraud, we note that the vast majority of such works are in the financial sector. In their treatises, researchers Kuzior A., Brożek P., Kuzmenko O., Yarovenko H., Vasilyeva T. [3] reveal the issues of countering the risks of cybercrime in financial institutions based on forecasting trends associated with the most popular cyberattacks; Kuzmenko O., Kubálek J., Bozhenko V., Kushneryov O., Vida I. [4] describe an approach to innovation management to protect the financial sector from cybercrime by analyzing large amounts of information; and others.

The study of cybercrime in the healthcare sector has its own peculiarities due to the specifics of the industry. Thus, technical and technical security threats in the field of healthcare are revealed by scientists Govindarajan U.H., Singh D.K., Gohel H.A. [1] – on predicting the landscape of cybersecurity threats and related technical trends in the field of telehealth using bidirectional coder representations; Singh H.J., Gupta S., Vyas S. [7] – on the basics of health data protection based on prevention methods. A separate study of cybersecurity based on blockchain technology stands out: Yazdinejad A., Rabieinejad E., Hasani T., Srivastava G. [10], who describe recommendation systems for secure supply chain management of cyber-physical products based on blockchain; Tadaka S.M., Tawalbeh L. [8], who apply blockchain in healthcare, industry, and cyber-physical systems. An important innovative direction is the use of artificial intelligence for the analysis and practical research of online health information, which is also described in Wagle V., Kaur K., Kamat P., Patil S., Kotecha K. [9] and others.

Purpose of the article. The main purpose of the study is a retrospective and current systematic bibliometric analysis of scientific research in the field of cyber fraud as a threat to the sustainable development of the health care system based on Scopus, VOS Viewer, Statista.

Summary of the main research material. The research was carried out in the following logical sequence: defining the criteria for selecting publications on cyber fraud in the healthcare system; determining the dynamics of scientific articles in this direction; alyzing the geographical distribution of research; studying the distribution of subject areas of the problem under study; forming and analyzing clusters of scientific articles on cyber fraud in the healthcare system by key terms; building an evolutionary and temporal map of the interrelationships of the studied categories with other scientific concepts in dynamics; identifying and analyzing the directions of distribution of cyberattacks in the healthcare sector by vectors based on the Statista database. The mechanisms for implementing this stage are the analytical tools of the Scopus platform, the VOS Viewer software, Statista statistical database.

According to the results of an electronic review of publications in the Scopus database for the period from 2012 to 2023, using the search terms: (("cyber fraud" OR "cyber security")), AND "healthcare system"; search string criteria: TITLE-ABS-KEY ("cyber fraud" OR "cyber security"), AND "healthcare system")), obtained as a result of the preliminary analysis of 110 publications on this topic.

Figure 2 shows the results of the dynamics of scientific articles in the Scopus scientometric database in the direction of cyber fraud in the healthcare system for the period from 2012 to 2023 based on the analytical tools of the Scopus platform.

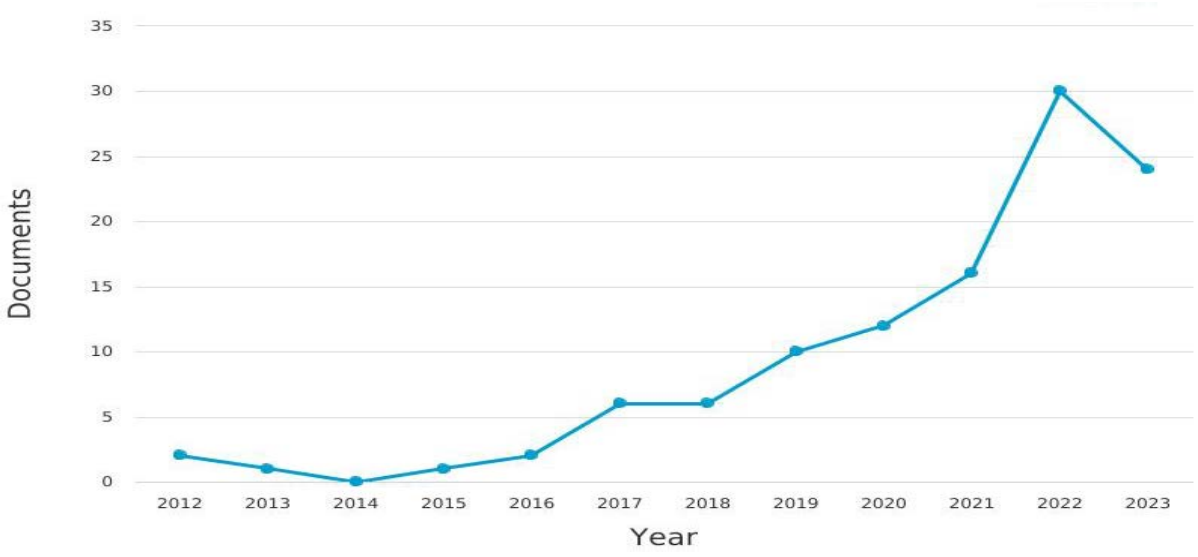

Figure 2 – Dynamics of scientific articles in the Scopus database in combination with the terms "cyber fraud" or "cyber security" and "healthcare system"

Source: systematized by the authors based on Scopus data

The data in Figure 2 clearly indicate a steady increase in the relevance of this area of research, namely, during 2014–2022, the number of publications in the Scopus database on this issue increased annually. Moreover, the rapid growth has been observed since 2019, respectively, in 2019 – 10 publications (9% of all publications), 2020 – 12 publications (11% of all publications), 2021 – 16 publications (15% of all publications), and the peak value in 2022 – 30 publications (27% of all publications).

Figure 3 presents the geographical distribution of studies combining the terms "cyber fraud" or "cyber security" and "healthcare system" in the context of the direction under study for the period 2012–2023, using the Scopus Toolkit. Moreover, the largest number of scientists working on this issue is in the following countries: India – 21 scientists (14%), United States – 15 scientists (10%), Saudi Arabia – 14 scientists (9%), United Kingdom – 12 scientists (8%), the average number of scientists: Italy – 6 scientists (4%), Finland and Greece – 5 scientists (3% each), China – 4 scientists (3%), scientists from other countries – from 1 to 3 scientists.

The distribution of the subject areas of the problem under study for the period 2012–2023, using the Scopus Toolkit (Figure 4), contains a wide range of interdisciplinary publications, which confirms the relevance of the chosen scientific direction [1; 4; 8; 9].

Thus, most publications on this issue belong to the following fields: "Computer Science" – 83 publications (32.9%) and "Engineering" – 60 publications (23.8%), the average number to "Medicine" – 24 publications (9.5%), "Decision Sciences" – 21 publications (8.3%), "Mathematics" – 18 publications (7.1%), less to "Social Sciences" – 10 publications (4.0%), "Physics and Astronomy" – 9 publications (3.6%), "Chemical Engineering" – 5 publications (2, 0%), "Chemistry" – 4 publications (1.6%), "Energy" – 4 publications (1.6%), other 5.6% ("Biochemistry-Genetics and Molecular Biology", "Business-Management and Accounting", "Materials Science" – 3 publications (1.2% each), "Health Professions" – 2 publications (0.8%), "Economics_ Econometrics and Finance", "Environmental Science", "Nursing" – 1 publication (0.4%)). Moreover, a third of the publications relate to related fields.

During the next two stages, research trends on cyber fraud in the healthcare system are identified using the tools of the VOSViewer software [4]. Based on the metadata of scientific publications in the Scopus database, clusters of scientific articles were formed and visualized using the keywords "cyber fraud" or "cyber security" and "healthcare system" for the period 2012-2023 (Figure 5). The study identifies six substantive clusters, each of which has connections with relevant phrases in scientific works and characterizes the areas of research included in the sample according to the established criteria.

As illustrated in Figure 5, the formed 6 clusters include, respectively, the following 50 scientific categories: Cluster 1 ("red", 14 items) – cyber security, cyber-attacks, cyber-security, cybersecurity, diagnosis, healthcare systems, internet of medical thing, internet of medical things (iomt), internet of things, intrusion detection, machine learning, malware, medical services, patient treatment; Cluster 2 ("green", 11 items) – block-chain, blockchain, COVID-19, cryptography, digital storage, health records, hospital data processing, interoperability, privacy, security, sensitive data; Cluster 3 ("blue", 10 items) – computer crime, crime, cyber-physical systems, data privacy, embedded systems, health care, health risks, healthcare sectors, medical computing, network security; Cluster 4 ("yellow", 7 items) – article, artificial intelligence, computer security, healthcare organizations, healthcare system, hospitals, human; Cluster

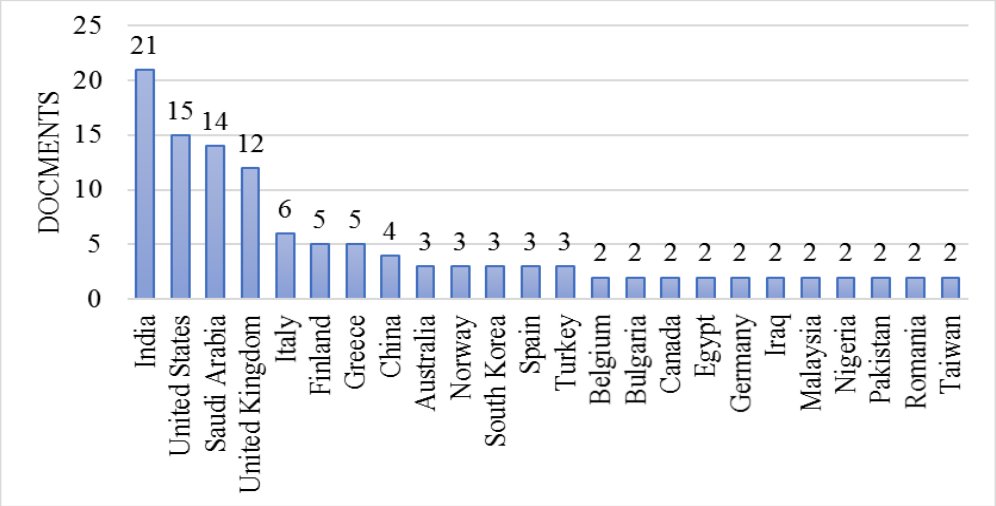

Figure 3 – Geographical distribution of scientific articles combining the terms "cyber fraud" or "cyber security" and "healthcare system"

Source: systematized by the authors based on Scopus data

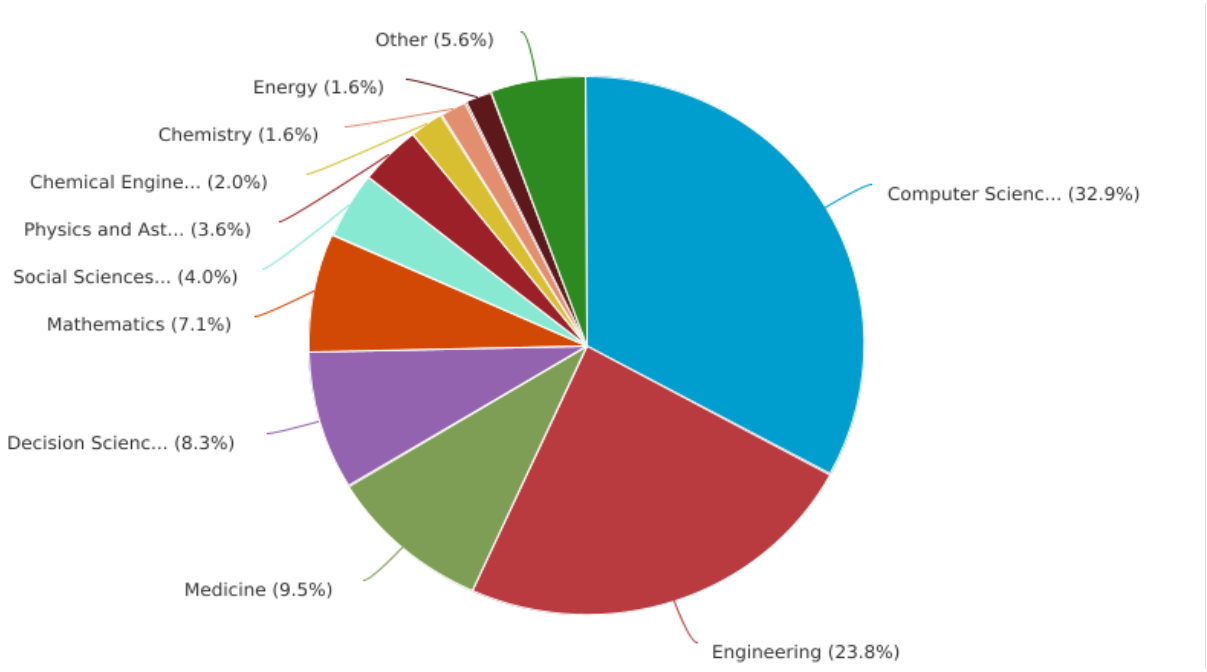

Figure 4 – Distribution of subject areas of scientific articles on cyber fraud in the healthcare system

Source: systematized by the authors based on Scopus data

5 ("purple", 5 items) – health-care system, healthcare industry, internet of things (iot), iot, security of data; Cluster 6 ("light blue", 3 items) – healthcare, information systems, information use.

The first, largest cluster combines research cybersecurity (cyber-attacks, concerning the study and protection against computer attacks; intrusion detection, concerning technologies and methods for detecting illegal intrusions into computer networks and systems), as well as medical technologies and IoT (Internet of Things) (diagnostics, concerning research on systems and technologies for establishing medical

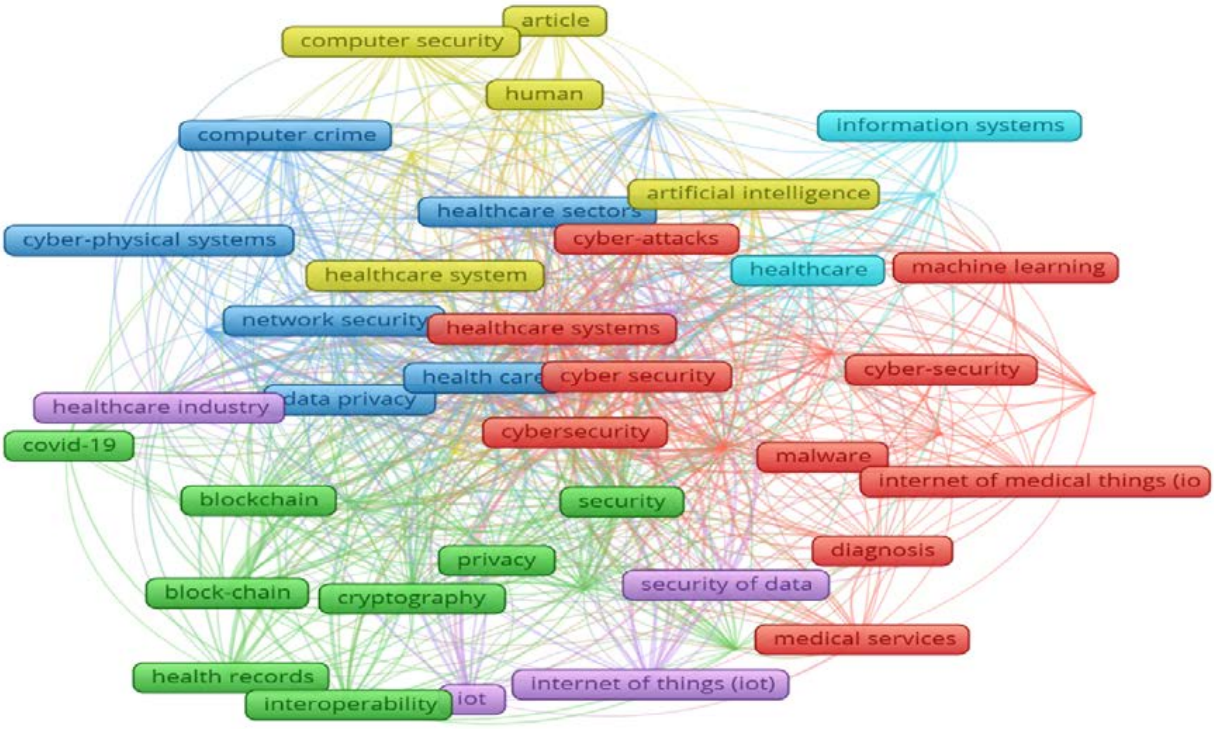

Figure 5 – Visualization of clusters of scientific articles on cyber fraud in the healthcare system by key terms "cyber fraud" or "cyber security" and "healthcare system" for the period 2012–2023

Source: formed by the authors via VOS Viewer

diagnoses; medical services, concerning the provision of medical services and patient care; Internet of Medical Things, concerning the use of IoT in the healthcare sector).

The second cluster of research specializes in the study of the blockchain technology for storing and processing medical data in the context of the COVID-19 pandemic (application of blockchain technology in the context of the COVID-19 pandemic to ensure safe and reliable storage of medical data; development of cryptographic standards and methods for protecting this medical data); privacy and security of medical data on the blockchain (development and application of standards and technologies that can ensure a high level of patient privacy while storing their medical data on the blockchain).

The scientific papers of the third cluster focus on a combination of research in two areas cybersecurity in healthcare (focuses on cybersecurity and data privacy issues in healthcare, including the aspect of computer crime affecting the healthcare sector, combining the study of the concepts of network security, data privacy, healthcare, medical computing, and cybercrime); Embedded Systems in Medical Technologies (focuses on the use of embedded systems and cyber-physical systems in medical technologies and computing, combining the study of the concepts of embedded systems, cyber-physical systems, healthcare, medical computing).

Scientific research in the fourth cluster specializes in combining peculiarities of artificial intelligence impact on information security in the healthcare sector (study of the results of the impact on information security of the use of artificial intelligence in the healthcare sector, which involves the analysis of possible risks, threats to the integrity and confidentiality of medical data, as well as the development of strategies, technologies, methods for protecting medical data in the context of healthcare institutions); specifics of the use of artificial intelligence in the management of medical institutions (studying the possibilities of using artificial intelligence to further optimize the management of medical institutions, analyzing opportunities to increase efficiency, automate processes, improve the quality of medical services in the healthcare sector through the use of intelligent technologies).

The fifth cluster includes research papers covering the following areas: ensuring and maintaining security in the Internet of Things (security of medical data in the healthcare system and in the healthcare industry; avoiding violations of the integrity of medical data and their proper confidentiality); digital transformations in healthcare (combining healthcare and the Internet of Things to improve healthcare services and preserve medical data; focusing on the use of IoT technologies and ensuring the security of medical data to create the latest medical systems).

In the sixth cluster, it combines scientific articles on e-health (development and introduction of information systems in the healthcare sector, such as electronic medical records, electronic information exchange between medical institutions, patient monitoring systems, telemedicine; use of information systems in the process of diagnosing and treating patients); analytics in the healthcare system (use of information systems to optimize processes in healthcare, management of medical systems, use of artificial intelligence technologies for disease prediction, optimization of resources in medical institutions, and treatment decisions).

The next stage is to build an evolutionary and temporal map of the interrelationships of the studied categories "cyber fraud" or "cyber security" and "healthcare system" of the area of cyber fraud in the healthcare system with other scientific concepts in the dynamics for the period 2012–2023 (Figure 6).

The results of the evolutionary and temporal analysis presented in Figure 6 show that in the dynamics from 2012 to 2023, three stages of change in the studied areas can be distinguished [2, 5]. Until 2019, research was mainly focused on identifying and detecting cybersecurity threats in healthcare systems. At the turn of 2020–2021, due to the growing number of cyberattacks on healthcare systems in the context of the COVID-19 pandemic, research was focused on preventing cyberfraud in the healthcare industry during COVID-19; finding new ways to protect medical data and medical infrastructure from cyberattacks. Starting in 2022, healthcare scientists will focus on studying the impact of artificial intelligence and the Internet of Things on cybersecurity and cyber defense in the healthcare system; on increasing awareness of cybercrime and cybersecurity among medical staff and patients.

The last stage of the study identified and analyzed the distribution of various cyberattacks in the healthcare sector worldwide for the period from October 2021 to September 2022 by main vectors [5] (Figure 7).

Figure 7 shows that the healthcare sector experienced various types of cyberattacks between October 2021 and September 2022, with network and application cybercrime accounting for the largest share (63% of all attacks); malware was the second most common type of attack (22%); account anomaly vector was the third (12%); social engineering was the fourth (3%); and policy violations were the least common (1%).

Conclusions. Cybertechnology allows criminals to remain anonymous, using high-tech methods to commit cyberattacks quickly and invisibly. According to the retrospective and current systematic bibliometric analysis of scientific research in the area of cyber fraud in the healthcare system, it is worth noting the logical sequence of the model by which the analysis is proposed: analyzing the geographical distribution of research; studying the distribution of subject areas

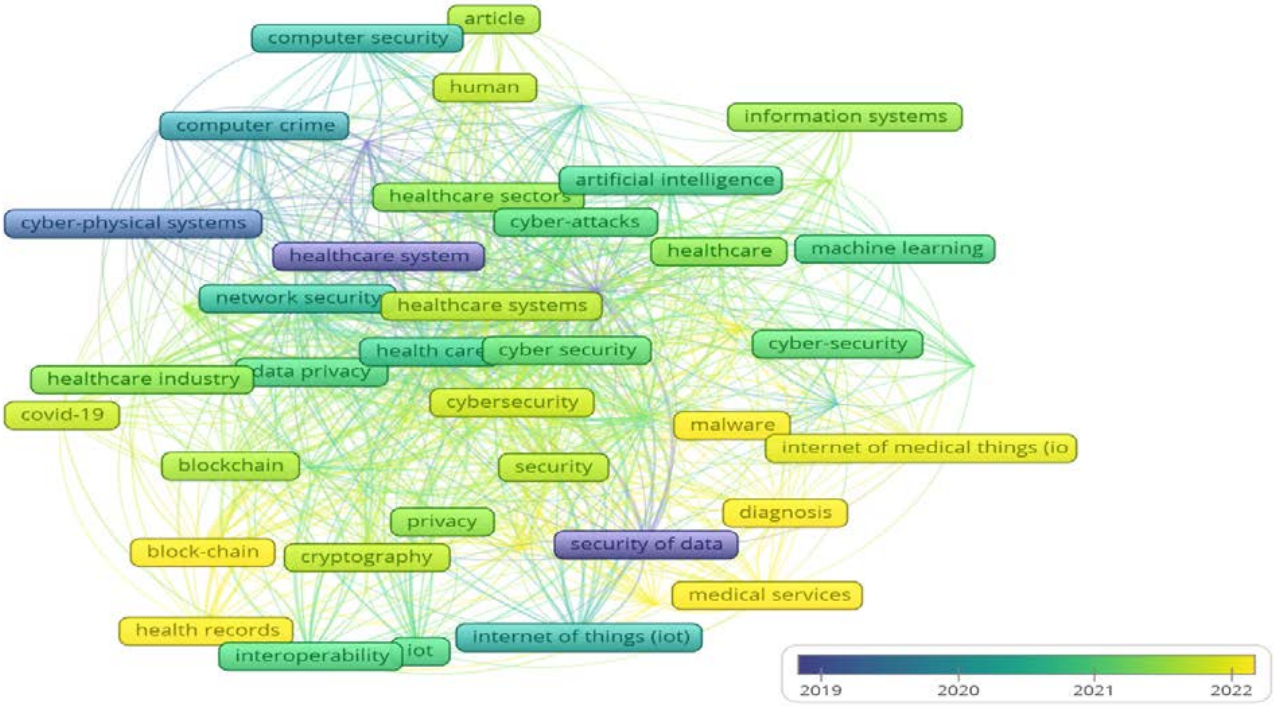

Figure 6 – Visualization of the evolutionary and temporal map of the interrelationships of the studied categories "cyber fraud" or "cyber security" and "healthcare system" clusters in scientific articles on cyber fraud in the healthcare system in the dynamics for the period 2012–2023

Source: formed by the authors via VOS Viewer

of the problem under study; forming and analyzing clusters of scientific articles on cyber fraud in the healthcare system by key terms; building an evolutionary and temporal map of the interrelationships of the studied categories with other scientific concepts in dynamics; identifying and analyzing the directions of distribution of cyberattacks in the healthcare sector by vectors.

The constant growth of the relevance of the studied area has been proved, with a rapid increase in 2019–2022. It is established that the largest number of scientists working on the issue is in the following countries: India (14%), United States (10%), Saudi Arabia (9%), United Kingdom (8%), Italy (4%). There was a wide interdisciplinarity of publications in the following areas: computer science (32.9%), engineering (23.8%), medicine (9.5%), decision sciences (8.3%), mathematics (7.1%), social sciences (4.0%), physics and astronomy (3.6%). Six clusters of scientific articles on cyber fraud in the healthcare system were formed and visualized, and three stages of change in the studied areas were identified. The most frequent types of cyberattacks in the healthcare sector around the world are identified: network and

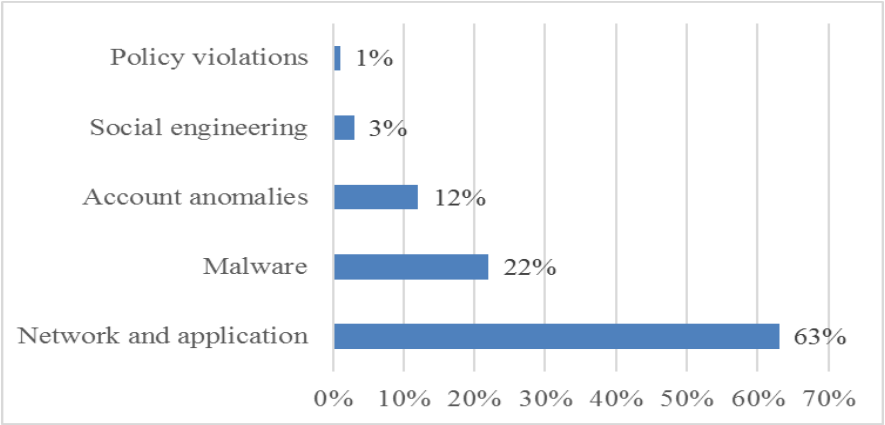

Figure 7 – Distribution of the most frequent types of cyberattacks in the healthcare sector worldwide for the period October 2021 – September 2022

Source: compiled by the authors

program intrusions (63%), malware (22%), account anomalies (12%).

To summarize, the application of the proposed model of a comprehensive systematic study of the healthcare industry will make it possible to identify priority areas and problematic aspects of the industry in terms of cybersecurity in a timely manner, improve the protection of patients, patient data, telemedicine systems, hospital security management, strengthen the protection of medical devices, and minimize the risks of cyber losses in the healthcare system.

References:

1. Govindarajan, U., Singh, D., & Gohel, H. (2023) Forecasting cyber security threats landscape and associated technical trends in telehealth using bidirectional encoder representations from Transformers (Bert). Computers'; Security, 133, 103404. DOI: https://doi.org/10.1016/j.cose.2023.103404

2. IBM. (February 24, 2023) Distribution of cyber attacks across worldwide industries in 2022 [Graph]. In Statista. Retrieved October 10, 2023, from https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

3. Kuzior A., Brożek P., Kuzmenko O., Yarovenko H., Vasilyeva T. (2022) Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends. *Journal of Risk and Financial Management*. 15(12): 613. DOI: https://doi.org/10.3390/jrfm15120613

4. Kuzmenko, O., Kubálek, J., Bozhenko, V., Kushneryov, O., Vida, I. (2021) An approach to managing innovation to protect financial sector againstcybercrime. *Polish Journal of Management Studies,* 24(2), 276–291.133–138. DOI: https://doi.org/10.17512/pjms.2021.24.2.17

5. Orange. (December 1, 2022) Distribution of cyber attacks in healthcare industry worldwide from October 2021 to September 2022, by type [Graph]. In Statista. Retrieved October 09, 2023, from https://www.statista.com/statistics/1362863/cyber-attacks-on-healthcare-organizations-worldwide-by-type/

6. Pujitha, K., Nandini, G., Sree, K. V., Nandini, B., & Radhika, D. (2023) Cyber hacking breaches prediction and detection using machine learning. 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN). DOI: https://doi.org/10.1109/vitecon58111.2023.10157462

7. Singh, H. J., Gupta, S., & Vyas, S. (2023) A prevention technique-based framework for securing healthcare data. Proceedings of Fourth International Conference on Computing, Communications, and Cyber-Security, 777–787. DOI: https://doi.org/10.1007/978-981-99-1479-1_57

8. Tadaka, S. M., & Tawalbeh, L. (2020) Applications of blockchain in healthcare, industry 4, and Cyber-Physical Systems. 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). DOI: https://doi.org/10.1109/iotsms52051.2020.9340215

9. Wagle, V., Kaur, K., Kamat, P., Patil, S., & Kotecha, K. (2021) Explainable AI for Multimodal Credibility Analysis: Case Study of Online Beauty Health (mis)-information. IEEE Access, 9, 127985–128022. DOI: https://doi.org/10.1109/access.2021.3111527

10. Yazdinejad, A., Rabieinejad, E., Hasani, T., & Srivastava, G. (2023) A Bert-based recommender system for secure blockchain-based Cyber Physical Drug Supply Chain Management. Cluster Computing. DOI: https://doi.org/10.1007/s10586-023-04088-6