https://doi.org/10.33271/nvngu/2022-5/174

T. A. Vasilyeva[1,2,3],
orcid.org/0000-0003-0635-7978,
O. V. Kuzmenko[1],
orcid.org/0000-0001-8520-2266,
N. V. Stoyanets[4],
orcid.org/0000-0002-7526-6570,
A. E. Artyukhov[1],
orcid.org/0000-0003-1112-6891,
V. V. Bozhenko[1,5],
orcid.org/0000-0002-9435-0065

1 – Sumy State University, Sumy, Ukraine, e-mail: v.bozhenko@uabs.sumdu.edu.ua
2 – Silesian University of Technology, Gliwice, the Republic of Poland
3 – The London Academy of Science and Business, London, the United Kingdom of Great Britain and Northern Ireland
4 – Sumy National Agrarian University, Sumy, Ukraine
5 – Tubingen University, Tubingen, the Federal Republic of Germany

THE DEPICTION OF CYBERCRIME VICTIMS USING DATA MINING TECHNIQUES

Purpose. Development of a scientific and methodological approach for creating a phase depiction of a cybercrime victim by identifying significant personified characteristics.

Methodology. In the process of research, methods of systematization, comparison, grouping, logical generalization, bibliometric analysis, regression analysis (the method of sigma-limited parameterization), and the algorithm of associative rules were used.

Findings. According to the results of the research, it was established that the countries with the highest rates of cyber fraud in the field of financial services include Luxembourg (15 %), France (14 %), Great Britain (13 %) and Denmark (11 %) are among. In 2020, on average, every *10th* resident of the European Union became a cyber victim when performing financial transactions. The results of an empirical analysis using the algorithm of associative rules showed that in 100 % of the analyzed cases of cyber fraud in the field of financial services among European residents, stable patterns are found between the following parameters: "a married woman who raises three children", "a woman aged 55–64 years old who raises three children", "a married person who periodically experiences financial difficulties and raises three children", "a person who lives in a rural area and raises three children", "a person aged 65–74, who has three children". In addition, the probability for a woman raising three children of becoming a victim of cyber fraud is 87.5 %. In 71.4 % of cybercrime cases in the field of financial services, a close causal relationship is traced with the following parameters: "manual worker who was cyberattacked through a smartphone", "a person who periodically experiences financial difficulties and a cyberattack occurred through a smartphone".

Originality. The use of profiling technology allows evaluating and predicting the behavior of the financial services consumer in the conditions of the growing risk of cyber fraud based on the systematization and establishment of cause-and-effect relationships between the most informative personalized signs of them.

Practical value. The development of a phase depiction of a probable victim of cybercrime in the financial system allows identifying the signs of a cyber threat in the early stages, and immediately reacting to it, thus neutralizing or minimizing the negative consequences. The results of the conducted research will have practical significance for the management of financial institutions and public organizations that specialize in training and raising the level of financial and digital literacy of citizens.

Keywords: *victim, cybercrime, associative rules, financial institutions*

Introduction. The rapid use of digital products in various spheres of activity, the increase in Internet payments, the transition to e-government services, the development of the fintech industry are signs of the digital transformation of economic and social relations. Accordingly, the issue of cyber protection of personal and financial data is one of the main threats to the reputation, security, and economy of the country. Hacker attacks can cause serious consequences in the physical space, as well as provoke the emergence of threats to the financial stability of the country. Siemens experts determined that 56 % of energy supply facilities reported at least one cyberattack that resulted in data loss or work stoppage [1]. Cyber-attacks lead to significant financial losses: theft of corporate information, theft of financial data, theft of money, violation of the terms of a trade agreement, or, in general, loss of business or contract. Cyber-attacks can cause reputational losses and undermine the trust of economic entities (contractors, consumers, etc.). This, in turn, can potentially lead to lost customers, lost sales, and reduced profits. In 2020, cybercrime losses in the US are estimated at $4.2 million, which is twice as much as in 2018 ($2.7 million).

Today, cybercriminals are technologically advanced groups that use modern information solutions: artificial intelligence, cloud technologies, powerful computer support, and others. Strengthening the efforts to reduce the number of cyber victims from financial transactions is impossible in isolation from the scientific support of the cyber protection system. The modern development of information technologies makes it possible to accumulate large datasets, process them and obtain scientifically based regularities, which should be taken into account when forming a system for preventing cyber threats in the financial sector. One of the leading directions in solving this task is the creation of the phase depiction of a probable cybervictim, which allows identifying the signs of a cyber threat in the early stages, and reacting accordingly, thereby neutralizing or minimizing the negative consequences.

Literature review. Ensuring cyber security is an ever-growing problem for critical infrastructure facilities and national regulators. Today, combating cyber threats is one of the main topics for discussion at international economic forums and conferences; this issue is widely investigated in the works of foreign scientists. Bibliometric analysis was used to examine trend and structural regularities of publication activity on cyber security issues. Scopus scientometric database was selected for analysis. In the search query, articles corresponding to the simultaneous consideration of such categories as "cybercrime" and "cyber threat and cyber security" were selected. For a more in-depth analysis, only those articles that belong to such thematic fields as "social sciences", "economics and finance" and "business, management, and accounting" were selected. The search tools of the Scopus scientometric database made it possible to identify 2,814 scientific articles on the analyzed topic from 2008 to 2022 (Fig. 1).

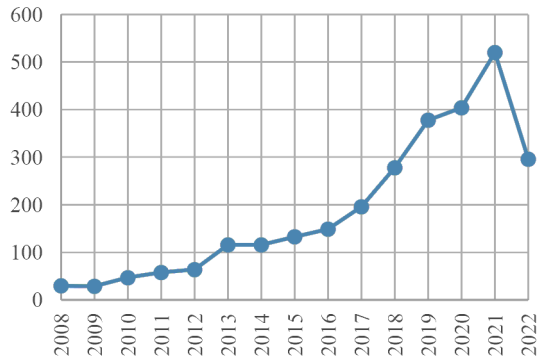

Fig. 1. Dynamics of scientific articles on cyber security indexed by the Scopus scientometric database

Fig. 1 shows that the significant popularity of this issue in scientific circles, as well as its permanent growth. A significant spike in publication activity on this issue was recorded in 2013 (116 publications), while in 2012 – 64 publications. In 2021, 520 articles devoted to the study on cyber threats in the context of social sciences and humanities were published.

During 2018–2022, the most active educational institutions whose scientists deal with this issue include: University of Oxford (22 articles published), The University of Texas at San Antonio (19 articles), University of Melbourne (16 articles), Deakin University (15 articles) and Universiteit Leiden (14 articles) (Fig. 2).

The analysis of the geographical structure of the affiliation of scientists with high publication activity in the field of cyber threats and cyber security in the context of social and humanitarian sciences only showed that the largest number of works on the specified topic were implemented by scientists from the USA (868 articles), Great Britain (379 articles), India (201 articles), Australia (156 articles) and China (110 articles).

Nowadays, enterprises, regardless of their industry affiliation, actively invest funds in the development of their information security and constantly monitor the internal system of combating cyber threats [2, 3]. In particular, the work by Al-Tahat and Moneim [4] analyzed the areas of practical application of neural networks and genetic algorithms in the information security management system of commercial banks. Berdyugin and Revenkov [5] developed, using Borland Delphi, software for quantitative assessment of the probability of cyberattack risk using electronic banking technology. Yarovenko, et al. [6] developed a methodology for assessing the risk of loss of information and knowledge due to violations in the company's information security. The work by Leonov, et al. [7] developed a prototype of the information system for suspicious transactions related to money laundering through banks based on the Structured Analysis and Design Technique in the DFD notation.

When forming a system for combating cybercrimes, it is important to monitor the behavioral patterns of both cybercriminals and cybervictims. In the article by Noor, et al. [8] constructed phase profiles of cyber fraudsters based on the analysis of their attack models by using the technique of distributed semantics of natural language processing. To identify suspicious operations in the information environment, biometric identification technologies are used [9, 10]. Yerdon, et al. [11] suggested using active eye tracking indicators to identify cyber fraudsters among employees of large companies. The work by Mousa, et al. [12] substantiated the need to strengthen information security among employees of financial institutions.

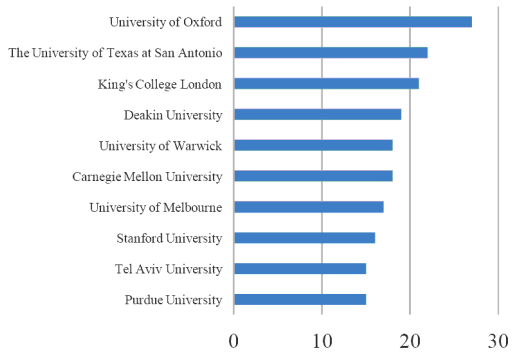

Fig. 2. Top universities whose scientists are engaged in cyber security

According to a group of scientists [13, 14], one of the factors of the rapid spread of cyber threats is the low level of digital and financial literacy, as well as insufficient awareness of the population about cyber-attacks and their potential destructive consequences. A significant number of cyberattacks are successfully implemented due to careless behavior in social networks [15]. In particular, the work [16] defines a set of cyber security skills of non-IT specialists that allow reducing risks to the information security of the company.

Increased ease of monetization of embedded financial and personal data as a result of cyberattacks is one of the reasons for the growth of cybercrime. An increase in the number of crimes in the information environment causes an increase in the scale of the shadow economy [17].

Purpose is the development of a scientific and methodological approach for creating a phase depiction of cybercrime by identifying significant personified characteristics.

Methods. To create a phase depiction of a cybervictim, a scientific and methodological approach has been developed, which involves the step-by-step implementation of the following steps:

1. Selection of the most relevant indicators characterizing cyber fraud using sigma-limited parameterization and Pareto diagram of t-values for GRM coefficients.

The Pareto chart allows you to visualize using the values of the Student's t-test of the priority of the indicators. This approach refers to one of the one-dimensional tests of significance.

2. Formation of a portrait of a victim of cybercrime based on taking into account significant personal characteristics identified using an algorithm of associative rules.

Associative rules are a very powerful technology that allows you to discover relationships between related events or elements. Generally, association rules are in the form of $X \Rightarrow Y$ where X and Y are the itemsets in the database. X is called an antecedent and Y is called a consequent [18, 19]. Associative rules are described in the form: $X \to Y$, $X \cap Y \to \varnothing$. Association rule mining consists of two basic measures and these are: support (s) and confidence (c).

Support: It is the probability that both X and Y will occur together in a transaction. Support ($X \to Y$) of the associative rule is a value equal to the ratio of the number of records $X \cup Y$ in the database D to the total number of records in the database.

Confidence: It is also the probability, but it follows a condition. In confidence, if a transaction has X, then it will also contains Y. Confidence to the associative rule is a value equal to the ratio of its support ($X \to Y$) to the support supp($X \to Y$) of the set X.

Support ($\{A, B\}$) = Number of Transactions (A, B).

Confidence ($A \Rightarrow B$) = Support (A, B)/Support (A).

Rules are generated in association rule mining using following two steps [18, 19]:

1. All the frequent itemsets are found using minimum support.

2. Using these frequent itemsets, strong association rules are generated, having confidence c above a predefined threshold value.

All calculations within the scope of this study were carried out in the Statistics software product.

Results. The use of profiling technology allows evaluating and predicting the behavior of the consumers of financial ser-

vices and is based on the systematization and establishment of cause-and-effect relationships between the most informative personalized characteristics. Remark that profiling technologies are a fairly common practice in law enforcement agencies to establish typical psycho types of criminals. In 2020 the special Eurobarometer survey was published that aimed at identifying EU citizens' awareness, experience, and perception of cyber security. The primary data of these survey was used for creating a phase depiction of cybercrime victim. 25 countries of the world were selected for analysis. IBM specialists [20] established that during 2018–2020, the most vulnerable sphere of activity to cybercrimes was the financial sector. Based on this, the creation of the phase depiction of the consumer of financial services as a cybercrime victim is based on the indicator "the share of the population that has encountered cyber fraud in the field of financial services" in the cross-section of European countries. The top countries with the highest rates of cyber fraud in financial services are Luxembourg (15 %), France (14 %), Great Britain (13 %), and Denmark (11 %). In 2020, on average, every 10th resident of the European Union became a cyber victim via financial transactions. 55 informational features were used based on data from 25 European countries to create a portrait of a likely cyber victim of a consumer of financial services.

The sigma-limited parameterization and a Pareto diagram of t-values for GRM coefficients are used to identify the most relevant indicators characterizing each of the 12 information features of the victim behavior. To build a Pareto chart using the sigma-limited parameterization method, it is necessary to additionally involve additional indicator – "persons who have encountered cyber fraud in the financial services" is chosen. The results of determining significant characteristics of the information feature "age" by constructing a Pareto diagram are presented in Fig. 3.

Table 1 presents all possible personal characteristics of a cyber victim and the results of selecting significant factors for creating a phase depiction of cybercrime victim.

After analyzing the survey data of citizens of the European Union regarding their attitude to cyber security issues, the following facts were identified:

- in 2020, the highest values of the cybercrime indicator in the field of financial services (21 %) were recorded for Lithuanian citizens aged 25–34 and Italian citizens aged over 75;

- the highest level of cyber fraud among consumers of financial services was recorded for the following spheres of their activity: persons studying (17 % – Hungary); freelancers (23 % – Denmark); managers (23 % – Ireland); other white collars (22 % – France); manual workers (17 % – Latvia); households (24 % – Bulgaria); unemployed (23 % – Denmark); retired (14 % – Great Britain); student (17 % – Hungary);

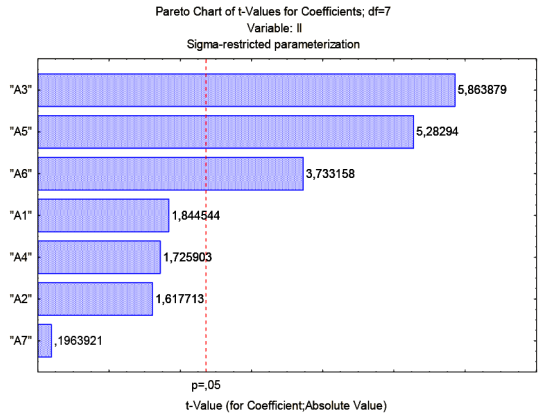

Fig. 3. Pareto diagrams of t-values of the significance of the influence of the information feature "age" on the performance indicator

Table 1

Input data for creating a phase depiction of cybercrime victim

Gender	man (G1)*; woman (G2)*
Age	15–24 years (A1); 25–34 years (A2); 35–44 years (A3)*; 45–54 years (A4); 55–64 years (A5)*; 65–74 years (A6)*; 75+ years (A7)
Socio-professional category	still studying (SPC1); self-employed (SPC2); managers (SPC3); other white collars (SPC4); manual workers (SPC5)*; house persons (SPC6); unemployed (SPC7); retired (SPC8); students (SPC9)
Marital status	married (MS1)*; single living with a partner (MS2)*; single (MS3); divorced or separated (MS4); widow (MS5)
Household situation	single household without children (HS1)*; single household with children (HS2); multiple household without children (HS3)*; household with children (HS4)*
Household composition	1 child (HC1)*; 2 children (HC2)*; 3 children (HC3)*; 4+ children (HC4)*
Difficulties paying bills	most of the time (DPB1); from time to time (DPB2)*; almost never/never (DPB3)*
Consider belonging to	the working class (C1); the lower middle class (C2)*; the middle class (C3)*; the upper middle class (C4); the upper class (C5)
Subjective urbanization	rural village (SU1)*; small/mid-size town (SU2)*, large town (SU3)*
Use of the Internet	every day (UI1)*; often/sometimes (UI2)*
Devices used to access the Internet	home computer (DAI1); laptop (DAI2); tablet (DAI3); smartphone (DAI4)*; TV (DAI5)*; game console (DAI6)
Aware of existence of portals/forms for reporting cybercrime	website (AEP1)*; email address (AEP2); online form (AEP3); contact number (AEP4); any other way (AEP5)

* statistically significant indicators

- among European countries, on average, 7 % of married persons became victims of cybercrime (while in France – 16 %, Latvia – 15 %); 8 % are single living with a partner (Italy, Romania – 14 %); 7 % – single (Latvia – 15 %, Great Britain – 13 %); 7 % – divorced (Great Britain – 20 %, France – 16 %); 9% – widow/widower (France – 21 %);

- households with children were more likely to become victims of cyber fraud when using financial services;

- among the top European countries whose persons became cyber victims in the field of financial services, depending on the composition of their families, we note the following: citizens of Lithuania who have one child (22 %); Danish citizens who have three children (20 %); French citizens who have four or more children (18 %);

- 12 % of average Europeans had difficulties paying their bills, and accordingly, they are more likely to become a victim of cyber fraud;

- average Europeans who consider themselves to belong to the upper class (33 %) more often became victims of illegal activities in virtual space compared to those persons who consider themselves lower on the social scale;

- the largest number of offenses related to the use of financial and moral damage in financial settlements is related to persons living in large cities: in Croatia – 22 % of citizens, France – 18 %, Belgium, Austria, and Great Britain – 15 %;

- an average of 13 % of residents of European countries became victims of cyber fraud due to the use of a game console, while in some European countries this figure is several times

higher: Romania – 37 %, the Czech Republic – 36 %, Hungary – 35 %. In addition to the game console, the survey found that on average 11 % of Europeans were exposed to cyber-attacks due to the imperfection of the protection system when making financial transactions through smart TVs, while in Romania – 27 % of citizens, Hungary – 26 %, Latvia – 21 %;

- only 13 % of residents of European countries are informed about ways to report a cyber-attack when making financial calculations. At the same time, it should be noted that in some European countries this indicator is critically low: Latvia – 1 %, Spain, Portugal, Slovakia – 4 %, Sweden – 5 %.

Having selected the relevant indicators for building a phase portrait of a potential cyber victim of a consumer of financial services by using associative rules. Association rule mining involves the use of unsupervised machine learning techniques to analyze data for patterns, or co-occurrences, in a database.

We have built a network of associative rules of causality of connections between indicators of the cyber vulnerability of consumers of financial services. To implement this stage, we will use the STATISTICA software product: the Data Mining/ Sequence, Association, and Link Analysis command. For making associative rules we set up the following parameters: minimal support = 20.0 %, confidence = 10.0 %, maximum size of an itemset = 10. We present the obtained results in Table 2.

Based on an in-depth analysis of statistical data on cyber fraud in the field of financial services through the construction of associative rules, the following conclusions can be drawn:

- in 100 % of the analyzed cases of cyber fraud in the field of financial services among residents of European countries, stable patterns were found between the following parameters: “a married woman who raises three children”, “a woman aged 55–64 who raises three children”, “a married person who periodically experiences financial difficulties and raises three children”, “a person who lives in a rural area and raises three children”, “a person aged 65–74 who has three children”;

Table 2

Fragment of identified associative rules

Body	=>	Head	Sup, %	Conf, %
0.019 < G2 ⇐ 0.039, 0.021 < MS1 ⇐ 0.042	=>	0.019 < HC3 ⇐ 0.040	20	100
0.011 < A5 ⇐ 0.034, 0.019 < HC3 ⇐ 0.040	=>	0.019 < G2 ⇐ 0.039	20	100
0.021 < MS1 ⇐ 0.042, 0.023 < DPB2 ⇐ 0.051	=>	0.019 < HC3 ⇐ 0.040	20	100
0.037 < SU1 ⇐ 0.059	=>	0.019 < HC3 ⇐ 0.040	20	100
0.016 < A6 ⇐ 0.035	=>	0.019 < HC3 ⇐ 0.040	20	100
0.019 < G2 ⇐ 0.039	=>	0.019 < HC3 ⇐ 0.040	28	87.5
0.056 < MS2 ⇐ 0.071	=>	0.053 < AEP1 ⇐ 0.087	20	83.3
0.019 < HC3 ⇐ 0.040, 0.023 < DPB2 ⇐ 0.051	=>	0.019 < G2 ⇐ 0.039	20	83.3
0.021 < MS1 ⇐ 0.042	=>	0.019 < G2 ⇐ 0.039, 0.019 < HC3 ⇐ 0.040	20	83.3
0.011 < A5 ⇐ 0.034	=>	0.019 < G2 ⇐ 0.039, 0.019 < HC3 ⇐ 0.040	20	83.3
0.023 < HS4 ⇐ 0.045	=>	0.019 < G2 ⇐ 0.039	20	83.3
0.021 < MS1 ⇐ 0.042	=>	0.019 < G2 ⇐ 0.039	20	83.3
0.011 < A5 ⇐ 0.034	=>	0.019 < G2 ⇐ 0.039	20	83.3
0.011 < A5 ⇐ 0.034	=>	0.019 < HC3 ⇐ 0.040	20	83.3
0.021 < MS1 ⇐ 0.042	=>	0.023 < DPB2 ⇐ 0.051	20	83.3
0.021 < MS1 ⇐ 0.042	=>	0.012 < HC2 ⇐ 0.033	20	83.3
0.023 < HS4 ⇐ 0.045	=>	0.021 < MS1 ⇐ 0.042	20	83.3

- the probability of becoming a victim of cyber fraud for a woman raising three children is 87.5 %;

- with a probability of 83.3 %, cause-and-effect relationships are traced between the following parameters: “a woman who periodically experiences financial difficulties and raises three children”, “a woman who has a child”, “a woman aged 55–64”, “a married person raising two children”, “a person living in a small town and raising two (three) children”;

- in 71.4 % of cases of cybercrime in the field of financial services, a close causal relationship is traced with the following parameters: “a manual worker who was cyberattacked via smartphone”, “a person who periodically experiences financial difficulties and cyberattack occurred via smartphone”.

Thus, the identified parameters using the algorithm of associative rules make it possible to determine the most vulnerable categories of the population that need enhanced informational and advisory assistance in increasing the level of their information security when carrying out financial transactions.

Conclusions. The mass introduction of digital technologies creates both additional opportunities for the development of economic entities and certain threats – leakage of confidential data, theft of funds, loss of reputation, etc. In order to effectively counter cyber threats and ensure the financially stable and uninterrupted functioning of economic entities, it is advisable to adopt a set of measures aimed at monitoring the components of their information security, combining the efforts of the national regulator and company managers to inform about real and potential cyber-attacks, as well as creating high-quality competencies in the field of information security by improving the qualifications of employees. The proposed technique for building a profile of a cyber victim allows one to identify the most vulnerable groups of the population and improve the level of their digital hygiene.

Acknowledgements. *This research was funded by the grant from the Ministry of Education and Science of Ukraine (No. s/r 0121U100467, 0122U000783, 0121U109559, 0121U109553).*

References.

1. *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?* (n.d.). Retrieved from https://assets.siemens-energy.com/siemens/assets/api/uuid:c723efb9-847f-4a33-9afa-8a097d81ae19/siemens-cybersecurity.pdf.

2. Lopez, B.S., & Alcaide, A.V. (2020). Blockchain, AI and IoT to Improve Governance, Financial Management and Control of Crisis: Case Study COVID-19. *SocioEconomic Challenges*, *4*(2), 78-89. https://doi.org/10.21272/sec.4(2).78-89.2020.

3. Obeid, H., Hillani, F., Fakih, R., & Mozannar, K. (2020). Artificial Intelligence: Serving American Security and Chinese Ambitions. *Financial Markets, Institutions and Risks*, *4*(3), 42-52. https://doi.org/10.21272/fmir.4(3).42-52.2020.

4. Al-Tahat, S., & Moneim, O.A. (2020). The impact of artificial intelligence on the correct application of cyber governance in Jordanian commercial banks. *International Journal of Scientific and Technology Research*, *9*(3).

5. Berdyugin, A.A., & Revenkov, P.V. (2020). Cyberattack risk assessment in electronic banking technologies (the case of software implementation). *Finance: Theory and Practice*, *24*(6). https://doi.org/10.26794/2587-5671-2020-24-6-51-60.

6. 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.

7. Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings*, *2422*, 297-307. Retrieved from http://ceur-ws.org/.

8. Noor, U., Anwar, Z., Amjad, T., & Choo, K.K.R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, *96*. https://doi.org/10.1016/j.future.2019.02.013.

9. Kuznetsov, A., Datsenko, S., Gorbenko, Y., Chupilko, T., Korneyev, M., & Klym, V. (2021). Experimental researches of biometric authentication using convolutional neural networks and histograms of oriented graphs. *2021 IEEE 4th International Conference on Advanced*

Information and Communication Technologies, AICT 2021 – Proceedings, 288-292. https://doi.org/10.1109/AICT52120.2021.9628932.
10. Njegovanović, A. (2018). Digital Financial Decision With A View Of Neuroplasticity/Neurofinancy/Neural Networks. *Financial Markets, Institutions and Risks*, *2*(4), 82-91. https://doi.org/10.21272/fmir.2(4).82-91.2018.
11. Yerdon, V.A., Lin, J., Wohleber, R.W., Matthews, G., Reinerman-Jones, L., & Hancock, P.A. (2021). Eye-Tracking Active Indicators of Insider Threats: Detecting Illicit Activity During Normal Workflow. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2021.3059240.
12. Mousa, M., Sai, A.A., & Salhin, G. (2017). An Exploration for the Motives behind Enhancing Senior Banker's Level of Organizational Resilience: A Holistic Case Study. *Journal of Intercultural Management*, *9*(4). https://doi.org/10.1515/joim-2017-0025.
13. Andreou, P.C., & Anyfantaki, S. (2021). Financial literacy and its influence on internet banking behavior. *European Management Journal, 39*(5). https://doi.org/10.1016/j.emj.2020.12.001.
14. Kuzior, A., Kettler, K., & Rąb, Ł. (2022). Digitalization of work and human resources processes as a way to create a sustainable and ethical organization. *Energies*, *15*(1). https://doi.org/10.3390/en15010172.
15. Kirichenko, L., Radivilova, T., & Anders, C. (2017). Detecting cyber threats through social network analysis: short survey. *SocioEconomic Challenges, 1*(1), 20-34. http://doi.org/10.21272/sec.2017.1-03.
16. Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*, *27*(1). https://doi.org/10.1108/ICS-11-2016-0088.
17. Tiutiunyk, I., Kuznetsova, A., & Spankova, J. (2021). Innovative approaches to the assessment of the impact of the shadow economy on social development: an analysis of causation. *Marketing and Management of Innovations*, *3*, 165-174. http://doi.org/10.21272/mmi.2021.3-14.
18. Kaur, J., & Madan, N. (2015). Association Rule Mining: A Survey. *International Journal of Hybrid Information Technology*, *8*(7), 239-242. https://doi.org/10.14257/ijhit.2015.8.7.22.
19. Kaur, C. (2013). Association Rule Mining using Apriori Algorithm: A Survey. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *2*(6), 2081-2084.
20. *X-Force Threat Intelligence Index 2021. IBM Security* (n.d.). Retrieved from: https://www.ibm.com/downloads/cas/M1X3B7QG.

Побудова портрету кібержертви з використанням технологій data-mining

Т. А. Васильєва[1,2,3], *О. В. Кузьменко*[1], *Н. В. Стоянець*[4], *А. Є. Артюхов*[1], *В. В. Боженко*[1,5]

1 – Сумський державний університет, м. Суми, Україна, e-mail: v.bozhenko@uabs.sumdu.edu.ua
2 – Сілезький технологічний університет, м. Глівіце, Республіка Польща
3 – Лондонська академія науки та бізнесу, м. Лондон, Сполучене Королівство Великої Британії та Північної Ірландії
4 – Сумський національний аграрний університет, м. Суми, Україна
5 – Тюбінгенський університет, м. Тюбінген, Федеративна Республіка Німеччина

Мета. Розробка науково-методичного підходу для побудови фазового портрету жертви кібершахрайства шляхом ідентифікації значимих персоніфікованих характеристик.

Методика. У процесі дослідження використовувались методи систематизації, порівняння, групування, логічного узагальнення, бібліометричного аналізу, регресійний аналіз (метод сигма-обмеженої параметризації) та алгоритм асоціативних правил.

Результати. За результатами дослідження встановлено, що до країн із найвищими показниками кібершахрайства у сфері фінансових послуг належать Люксембург (15 %), Франція (14 %), Великобританія (13 %) і Данія (11 %). У 2020 році у середньому кожний 10-й житель Європейського Союзу став кібержертвою при здійсненні фінансових транзакцій. За результатами проведеного емпіричного дослідження з використанням алгоритму асоціативних правил встановлено, що у 100 % аналізованих випадків кібершахрайств у сфері фінансових послуг серед жителів європейських країн виявлені стійкі закономірності між такими параметрами: «заміжня жінка, яка виховує трьох дітей», «жінка у віці 55–64 роки, яка виховує трьох дітей», «заміжня (одружена) особа, яка періодично відчуває фінансову труднощі й виховує трьох дітей», «особа, яка проживає в сільській місцевості та виховує трьох дітей», «особа у віці 65–74 роки, яка має трьох дітей». Крім цього, ймовірність стати жертвою кібершахрайства жінці, яка виховує трьох дітей, становить 87,5 %. У 71,4 % випадків кіберзлочинності у сфері фінансових послуг прослідковується тісний каузальний зв'язок із такими параметрами: «працівник фізичної праці, у якого кібератака відбулася через смартфон», «особа, яка періодично відчуває фінансові труднощі й кібератака відбулася через смартфон».

Наукова новизна. Використання технології профайлінгу дозволяє оцінити та спрогнозувати поведінку споживача фінансових послуг в умовах зростаючого ризику кіберщахрайств на основі систематизації та встановлення причинно-наслідкових зв'язків між найбільш інформативними персоніфікованими їх ознаками.

Практична значимість. Розробка фазового портрету ймовірної жертви кібершахрайства у фінансовій системі дозволяє ідентифікувати ознаки кіберзагрози на ранніх етапах, відповідно відреагувати на неї, тим самим нейтралізувати або мінімізувати негативні наслідки. Результати проведеного дослідження матимуть практичну значимість для менеджменту фінансових установ і громадських організацій, що спеціалізуються на навчанні й підвищенні рівня фінансової та цифрової грамотності громадян.

Ключові слова: *жертва, кіберзлочинність, асоціативні правила, фінансові установи*

The manuscript was submitted 12.05.22.