Електронне наукове фахове видання **"Ефективна економіка"** включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України від 11.07.2019 № 975)
www. economy.nayka.com.ua | № 5, 2020 | 28.05.2020 р.

DOI: 10.32702/2307-2105-2020.5.11

УДК: 330.46:004.7.056.5

O. Kuzmenko
Doctor of Economic Sciences, Associate Professor,
Head of the Department of Economic Cybernetics, Sumy State University, Ukraine
ORCID ID: 0000-0001-8520-2266
N. Pilina
Postgraduate student, Department of Economic Cybernetics, Sumy State University
ORCID ID: 0000-0003-3381-5268
R. Pilin
Postgraduate student, Department of Economic Cybernetics, Sumy State University, Ukraine
ORCID ID: 0000-0003-1526-2583

TRENDS OF FRAUD OPERATIONS ON THE BANKING MARKET AND APPROACHES OF CYBERSECURITY ASSESSMENT

О. В. Кузьменко,
д. е. н., професор, завідувач кафедри економічної кібернетики,
Сумський державний університет
Н. В. Піліна,
аспірант кафедри економічної кібернетики,
Сумський державний університет
Р. В. Пілін,
аспірант кафедри економічної кібернетики,
Сумський державний університет

ТЕНДЕНЦІЇ ШАХРАЙСЬКИХ ОПЕРАЦІЙ НА БАНКІВСЬКОМУ РИНКУ ТА ПІДХОДИ ДО ОЦІНКИ КІБЕРБЕЗПЕКИ

The article emphasizes the identification of current trends in fraudulent transactions in the banking market. It is revealed the critical factors of cybercrime development in the financial sector. To analyze research on trends in fraudulent transactions in the banking market and approaches to assessing cybersecurity, a map of scientific bibliography is formed using the software product VOSviewer, based on Scopus database publications in terms of the intersection of queries in such categories as "banking" and "cybersecurity." Cybersecurity problems in banks, types of cyber fraud, and types of software that have been developed and implemented in recent years. It is presented a graphical visualization of the main risks, the growth of which is expected soon. It is formed the rating of the most common types of fraud in banks. The article is stressed on a structural analysis of priority sources of cyberattacks in the banking market. It is described options for malicious software to interfere with banking programs. The relevant requirements for building a system of counteraction within the internal processes of the bank are considered. Emphasis is placed on incidents

of making an adequate organizational structure, educational work with staff in the field of information security and risk management, the use of modern technologies, creating an effective management system and decision-making. It is conducted a comprehensive analysis of the bank's customer service channels, most prone to cybercrime attacks. The investigation is stressed on restrictions designed to protect bank accounts from unauthorized access. The article contains a list of problems that may arise in the bank's customers when using the affected software, which forces banks to implement anti-fraud systems. It is considered the latest approaches to countering bank account attacks. The article contains malicious software (Ramnit, Trickbot, Ursnif, Gustuff, IcedID, IcedID, Panda, Zevs), which has affected banks in recent years, causing significant material damage. Modern approaches to the assessment of the information protection system in general and cybersecurity, in particular, are identified.

У статті робиться акцент на ідентифікації сучасних тенденції шахрайських операцій на банківському ринку. Розкриваються ключові фактори розвитку кіберзлочинності в фінансовому секторі. Для аналізу досліджень тенденцій шахрайських операцій на банківському ринку та підходів до оцінки кібербезпеки сформовано карту наукової бібліографії за допомогою програмного продукту VOSviewer, що ґрунтується на публікаціях бази даних Scopus в розрізі перетину запитів за такими категоріями як «банківська справа» та «кібербезпека». Розглядається проблема кібербезпеки у банках, різновиди кібершахрайств та види програмних засобів, які розроблялися і впроваджувалися впродовж останніх років. Надана графічна візуалізація основних ризиків, зростання яких очікується в найближчій перспективі. Проведене рейтингування найбільш поширених видів шахрайств у банках. Проведений структурний аналіз пріоритетних джерел кібератак на банківському ринку. Описані варіанти втручання зловмисного програмного забезпечення у банківські програми. Розглядаються ключові вимоги до побудови системи протидії в межах внутрішніх процесів банку. Акцентується увага на інцидентах побудови адекватної організаційної структури, освітньої роботи з персоналом у сфері інформаційної безпеки та управління ризиками, використання сучасних технологій, побудови ефективної системи управління та прийняття рішень. Проведено комплексний аналіз каналів обслуговування клієнтів банку, найбільш схильних до атак кіберзлочинців. Розглядаються обмеження, покликані захистити банківські акаунти від незаконного доступу. Представлено перелік проблем, які можуть виникнути у клієнтів банку при використанні уражених програмних засобів, що змушує банки впроваджувати протишахрійські системи. Акцентується увага на новітніх підходах протидії атаки банківскьких рахунків. Розглядається зловмисне програмне забезпечення (Ramnit, Trickbot, Ursnif, Gustuff, IcedID, IcedID, Panda, Zevs), яке торкнулося банків останні роки, спричиняючи їм значні матеріальні збитки. Ідентифіковано сучасні підходи до оцінки системи захисту інформації в цілому та кібербезпеки зокрема.

***Keywords**: cybercrime, cyber fraud, cybersecurity, anti-fraud systems, malware.*

***Ключові слова**: кіберзлочинність, кібер-шахрайство, кібербезпека, системи протидії шахрайству, зловмисне програмне забезпечення.*

Formulation of the problem in general form and its relation to important scientific or practical tasks:

The relevance of the issue of the theft from bank accounts is beyond doubt. Attackers are developing ways to intrude banking systems, successfully neutralizing security programs, and appropriating considerable sums of money for themselves. According to experts, fraudsters get annually from 5% to 12% of gross income through misappropriation of money. World-famous companies claim corporate fraud as a phenomenon that exists in all countries around the globe. Damage resulting in increased expenses and decreased revenues is accompanied by the brand damage and loss of customers, which can further lead to the rating downgrade and even bankruptcy.

The number of cybercrimes is increasing every year. Therefore, the development of the information security industry is an important task both for the banking sector and for all companies with access to confidential information. Particular attention should be paid to securing data storage and data protection. Typically, malware is designed to gain access to personal, sensitive and other confidential information. Thus, in modern conditions of cybercrime develop-

ment, the problem of developing and introducing information protection systems in the banking sector based on the active automation of its business processes is especially relevant and requires effective measures to solve it.

An analysis of the latest research and publications in which the problem is solved and which the author relies on, the selection of previously solved parts of the general problem to which this article is devoted:

Analysis of peculiarities of development of financial and economic relations and active development and improvement of banking software product of functioning of market infrastructure allowed to distinguish some of the most explored factors of influence on security of banking software.

In the literature investigated software development of cybercriminals, which are created to interfere with banking software products. [1, 2, 3, 4, 5, 6, 7, 8] The most widespread cyber-attacks on banks, on cloud-technology and the ideas of protection against them are considered. [9, 10, 11, 12, 13] Particular attention is paid to Trojan malicious banking programs. [14,15, 16, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28]

To analyze research on trends of fraud operations on the banking market and approaches of cybersecurity assessment, a map of the scientific bibliography was formed using the software product vosviewer (vosviewer, 2020). It was based on data from publications selected in conjunction with cybersecurity and banking issues and generated in the Scopus database.

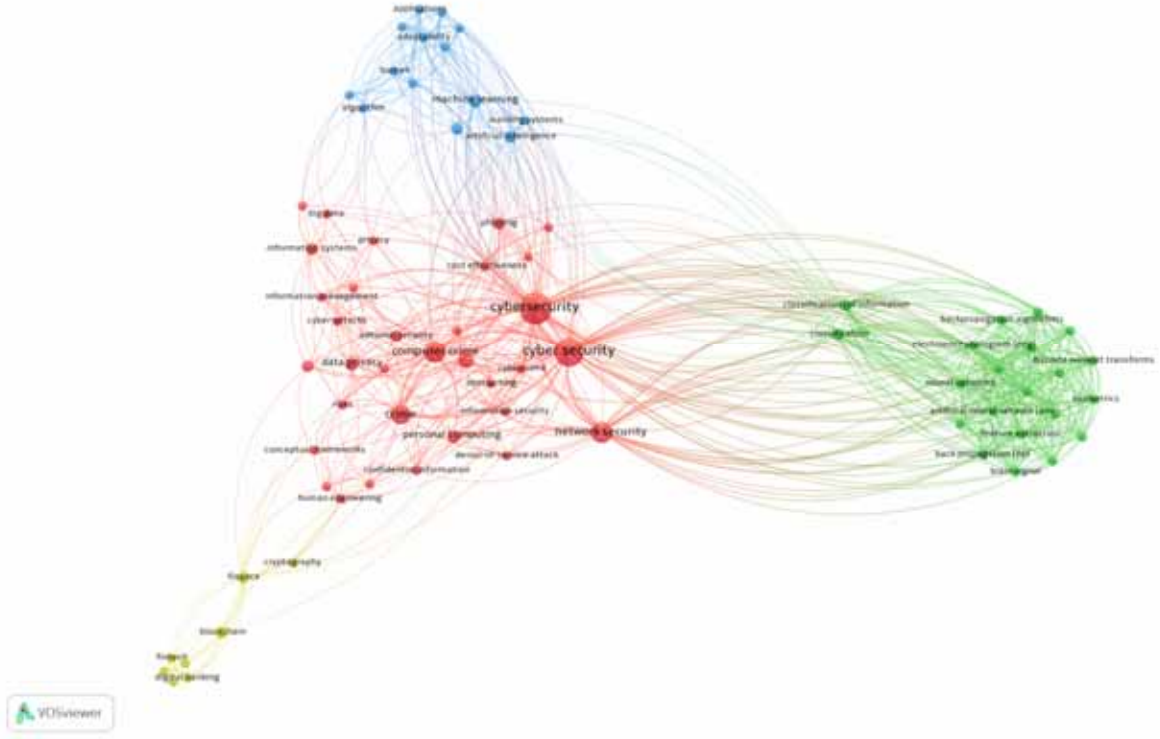

Figure 2 - Results of bibliometric analysis of scientific works on banking and cybersecurity theory for 2002–2019 in publications indexed by Scopus scientometric database (VOSViewerv.1.6.10 toolkit)

By researching Figure 1, we can understand that cyberattac, computer crime and security problems is a long time problem and scientists are actively working to solve the problem. The map shows clusters of publications by keywords, which are also combined with the data. As a result, 4 clusters of keywords were identified, each of which was distinguished by a color different from the others.

Researchers examining banking and cybersecurity issues study them in conjunction with network security, computer crime, risks, information management, big data—these categories formed in the first cluster. The second cluster emerged **blockchain**, digital banking, fintech and cryptography, that means program-technology point of investigated issue. Turning to the analysis of the next third cluster we have to consider its direction on machine learning, algorithm, artificial intelligence, which stressed on business-analytics and business intelligence of the point. And the last claster are formed by such categories as artificial neural network, discrete wavelet transforms, classification which are based on mathematical background of the research.

The goals' formulating of the article (Problem statement):

To identify relevant trends in banking fraud and approaches to the development and implementation of cyber security measures.

The basic results of the researches with full justification of scientific results:

Today there are many problems in business and, accordingly, in the banking sector. Rating agencies annually publish the most anticipated threats for the current year. According to the forecasts of Protiviti Inc. in Executive Perspectives on Top Risks for 2020, [1, page 7] the main risks for business in 2020 will be the following problems:

Top Risks for 2020 in business:

1. Impact of regulatory change and scrutiny on operational resilience, products and services
2. Economic conditions impacting growth
3. Succession challenges; ability to attract and retain top talent
4. Ability to compete with “born digital” and other competitors
5. Resistance to change operations
6. Cyber threats
7. Privacy/identity management and information security
8. Organization’s culture may not sufficiently encourage timely identification and escalation of risk issues
9. Sustaining customer loyalty and retention
10. Adoption of digital technologies may require new skills or significant efforts to upskill/reskill existing employees (new in 2020) [2]

Thus, cybersecurity and privacy issues are ranked 6th and 7th among the most anticipated 2020 issues.

Among Short-Term Risk Outlook, cyber-attacks in the form of data and money theft are among the top five issues of 2019, according to the article The Risks-Trends Interconnections Map 2019 [3, page 12].

Cyber dependency is steadily increasing due to the digital interconnection of people, things and organizations. This, in turn, can lead to bilateral or multilateral disputes between states, which may transform into an economic one (such as trade/currency wars, nationalization of resources), military, cyber, social, or other conflict. Large-scale cyber-attacks or malware cause major economic damage, geopolitical tensions, or widespread loss of trust in the Internet. In the Global Risks Report 2019, 14th Edition, which was presented at the International Economic Forum, cybersecurity has gained about 80% relevance among global threats. The data is presented in the chart Top Risks Expected to Increase in 2019.

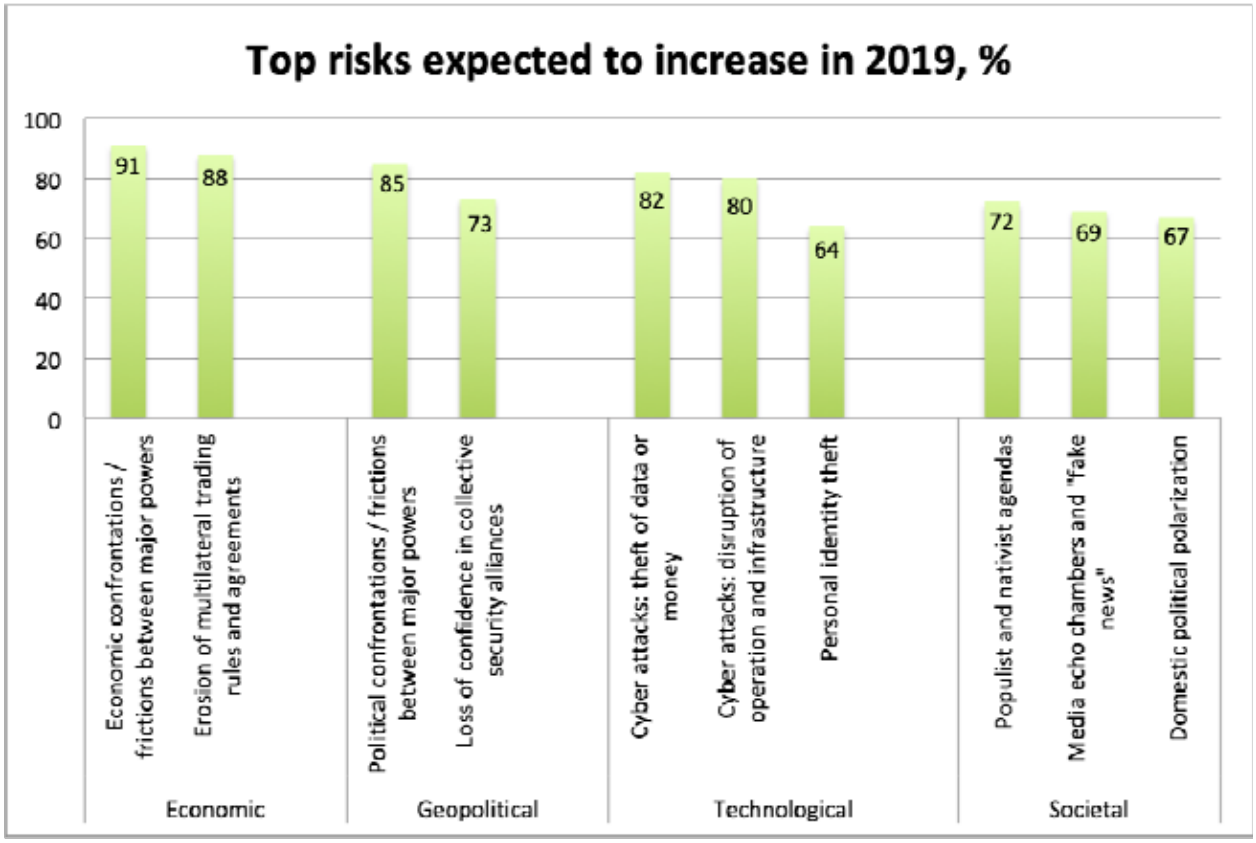

Figure 2 - Top Risks Expected to Increase in 2019

This is a confirmation of the high level of the problem for business and the banking sector as a whole.

In this part of the article, we consider the intrusion of cybercriminals into banking programs that contain confidential personal information of the client in the form of personal data, bank accounts, bankcard data, etc. Cybercriminals have at their disposal many software tools to commit illegal actions: viruses (classic file viruses, ransomware virus), Trojans, spies, hacking of an account, phishing, DDoS attacks, botnets, backdoor, worms, malware, rootkit, fraud, flood, etc.[4] Criminals also create programs using the latest machine learning technologies.[5]

One of the options for spreading cybercrime is the involvement of the so-called insiders — employees who knowingly participate in fraudulent activities within the organization, have certain advantages, endowed with legal authority and can easily gain access to classified information. Practice shows that the success of an attack depends directly on the presence of an employee in the company, which facilitates its implementation.

The following table shows the percentage of various types of fraud of the total top five in US banks, New York, 2018.

Top 5 most common types of fraud in US banks, 2018. According to Federal Trade Commission, Consumer Sentinel Network. [6, 7]

Table 1.

Type of fraud	Number of reports	Percent of total top five,%
Credit card fraud — new accounts	130,928	40.5
Miscellaneous identity theft*	87,765	27.1
Tax fraud	38,967	12.0
Mobile telephone — new accounts	33,466	10.3
Credit card fraud — existing accounts	32,329	10.0
Total	323,455	100

**Includes online shopping and payment account fraud, email and social media fraud, insurance and securities account fraud, and other identity theft.*

Thus, it is possible to conclude that more than half of all frauds in New York banks are credit card fraud and identity theft.

One of the ways to solve the issue of data protection in banks is to build a fraud-monitoring system. The quality of the cyber defense system is very important. It should not interfere with the work of the bank or company. The approach to the development of anti-fraud systems should be complex and cover the internal processes of the bank. It is very important to build an adequate organizational structure and to carry out educational work with personnel in the field of information security and risk management, to use modern technologies, build an effective management and decision-making model for incidents identified.

According to a 2017 survey, it takes about 214 days for a company to detect cyberattacks, and another 77 to resolve the problem. About 70% of attacks involve money theft, 26% focus on data theft.[8] Such a slow response to cyber threats can lead to significant material damage.

Currently, banks provide various types of customer service channels: mobile banking, Internet banking, ATMs, card payments, telephone service, and services at bank branches. Each individual option of working with a client's bank account is attacked by cybercriminals. Banks install anti-fraud systems to protect the system from attacks. It is important for the bank to choose a quality company that will develop and update the software, maintain the system in online mode, respond timely to unauthorized interventions, customer complaints, etc. This system costs a lot of money and requires constant investment to keep it running.

Certain limitations designed to improve service are a problem in banking anti-fraud systems. Such restrictions give only a temporary effect. Attackers easily bypass such limitations, but these limitations complicate access of an ordinary user to a bank account and actions with a card. The most common options for protecting an account from unauthorized access is user recognition by sending SMS with a unique code; limiting the number of purchases with one bank card by one user for a specified period of time; limits on the maximum amount of a single purchase by one user for a certain period of time; restrictions on the use of the number of bank cards by one user; limiting the number of users using bank cards that are tied to one bank account (family account); account history of purchases by bank cards, etc.

Restrictions may be imposed by each individual bank on its customers in order to protect users' funds and personal data. However, for clients, such a limit usually makes it difficult to access their own accounts.

We provide a list of the top malware for banks in the first half of 2019.

Turning to malware in the banking sector we have to mention that Agent Smith is a virus that has replaced the Android application code on 25 million devices. As of August 2019, AgentSmit hit around 22,000 devices across Ukraine, highlighting the need and priority of problem identification and software development that can protect banks from such a strong cybercrime impact. [9,10]

Anubis is a Trojan designed for Android mobile phones. It received additional features including the Remote Access Trojan (RAT) function, keylogger lock function, audio recording capability and various software features. It has been discovered and reported in hundreds of different Google Store applications. [11 Pandalab, про Anubis 12]

Asacub is a mobile banker distributed via phishing SMS containing a link that downloads a Trojan APK to an affected device. Asacub was first introduced in 2015 as spyware. Currently, Asacub functions as a banker to collect information about the victim's bank account. It can distribute incoming SMS messages, revealing browser history and contacts, executing remotely sent commands, intercepting messages, switching off the phone or its screen. [13, 14]

Bancos – Bancos steals financial information by using logs to capture the victim's data as they are uploaded to the destination banking website. Bancos may also supplement or replace a webpage with fields for entering personal and logon account information into a fake webpage. [15, 16]

Emotet is an advanced, self-propagating and modular Trojan. Emotet used to be a banking Trojan and has recently been used as a distributor of other malware. It uses several methods to maintain stability and avoid detection. It can also be spread through phishing spam emails containing malicious tabs or links.[17]

Ramnit is a banking Trojan that steals bank customer accounts, FTP passwords, session cookies, and personal information.[18]

Trickbot is a dominant banking Trojan that is constantly replenished with opportunities, features and distribution vectors. This allows Trickbot to be flexible and customized malware that can be distributed through multi-purpose campaigns. [19]

Ursnif is a Trojan that runs on the Windows platform. It is usually distributed through sets of exploits – Angler and Rig. It may steal information related to Verifone Point-of-Sale (POS) payment software. For this purpose, the Trojan communicates with a remote server to download the collected information and receive instructions. It then downloads the files to the infected system and executes them.[20, 21]

Gustuff is a Trojan Android banking introduced in 2019. It can target the customers of over 100 leading international banks, users of cryptocurrency services of popular websites and e-commerce markets. Gustuff can also create messaging files between Android and PayPal, Western Union, eBay, Walmart, Skype, and more. Gustuff may include a mechanism to use the Android Access Service to circumvent the security measures used by banks to protect against previous generations of mobile Trojans. [22]

IcedID is a banking Trojan that first appeared in September 2017, and is typically used by other well-known banking Trojans to expand its distribution potential, including Emotet, Ursnif and TrickBot. IcedID steals users' financial data through redirect attacks (installs a local proxy server to redirect users to counterfeit clone sites) and web injection attacks (overlays counterfeit content on top of the original page in the browser). [23, 24]

Necurs is one of the largest spam botnets in 2016, consisting of approximately 6 million bots. Today, the botnet is used to distribute many variants of malware, mainly banking Trojans and spies. [25]

Panda is a Zeus variant that is distributed through Exploit Kits. Since its development, Panda has focused on financial services in Europe and North America. A large-scale piracy campaign against Brazilian banks was registered before the 2016 Olympic Games. [26]

Ginp is a bank Android Trojan created on the basis of Anubis Trojan that is used to collect and steal sensitive information. [27] The latest version of Ginp has the same capabilities as most other Android banking Trojans: sending, collecting, SMS forwarding; collecting contact lists; call forwarding; switching between C&C (Command & Control) servers; keeping track of all software installed on the affected device; hiding the application icon; prevention of removal; emulation-detection; the ability to overlay a fake page on top of legitimate banking applications and portals to obtain user credentials entered into fraudulent fields. [28]

The conclusions of this research and perspective of further research in this area:

Cybercrime is a global problem of our millennium. Cybercriminals have many options for banking software interventions, and are constantly developing new programs and upgrading existing ones. To combat cybercrime, banks are implementing information security systems that cost a lot of money. This reduces banks' profits and causes them to be constantly in a state of readiness for cyberattacks. Therefore, developing and implementing qualitative software is an important task for the banking system worldwide.

The publication contains the results of the taxpayer-funded researches: № 0118U003574 “Cybersecurity in the banking frauds enforcement: protection of financial service consumers and the financial and economic security growth in Ukraine”, used in Sumy State University.

Література.

1. Goldsmith, D., Grauer, K. & Shmalo, Y., (2020), “Analyzing hack subnetworks in the bitcoin transaction graph”, *Applied Network Science*, vol. 5.

2. Protiviti Inc., “Executive perspectives on top risks for 2020”,[Електронний ресурс]. – Режим доступу: https://www.protiviti.com/CA-en/insights/protiviti-top-risks-survey ,(Accessed 15 May 2020).

3. Bormann, C., Castellani, A.P., Shelby, Z. (2012), “CoAP: An application protocol for billions of tiny internet nodes”, *IEEE Internet Computing*, art. no. 6159216, pp. 62-67., doi: 10.1109/MIC.2012.29.

4. Pons, P., (2013) “Computing communities in large networks using random walks”, *Internet measurement conference*, Barcelona, Spain, pp. 127-140.

5. Nwankwo, W., Ukaoha, K.C. (2019), “Socio-technical perspectives on cybersecurity: Nigeria’s cybercrime legislation in review”, *International Journal of Recent Technology and Engineering,* Volume 8, Issue 10, Pages 47-58, [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/337033615_Socio-Technical_Perspectives_On_Cybersecurity_Nigeria's_Cybercrime_Legislation_In_Review, (Accessed 15 May 2020).

6. Sharma, K., Bhasin, S., Bharadwaj Nalini, P. (2019), “A worldwide analysis of cyber security and cyber crime using twitter”, *International Journal of Engineering and Advanced Technology*, Volume 8, Issue 6 Special Issue 3, Pages 1051-1056, [Електронний ресурс]. – Режим доступу: https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13330986S319.pdf, (Accessed 12 May 2020).

7. Insurance Information Institute, (2020), “Facts + Statistics: Identity theft and cybercrime”, [Електронний ресурс]. – Режим доступу: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime, (Accessed 15 May 2020).

8. Shalaginov, A., Kotsiuba, I., Iqbal, A. (2019), “Cybercrime Investigations in the Era of Smart Applications: Way Forward Through Big Data”, *IEEE International Conference on Big Data*, Los Angeles; United States; 9-12 December 2019, Category number CFP19BGD-ART; Code 157991.

9. NetGuardians, (2020), “Digital banking fraud: Best practice for technology-based prevention”, [Електронний ресурс]. – Режим доступу: https://netguardians.ch/digital-banking-fraud/, (Accessed 15 May 2020).

10. Shishkova T., (2018), “The rise of mobile banker Asacub”, *Kaspersky,* [Електронний ресурс]. – Режим доступу: https://securelist.com/the-rise-of-mobile-banker-asacub/87591/, (Accessed 15 May 2020).

11. Thejas, G.S., Boroojeni, K.G., Chandna, K., Bhatia, I., Iyengar, S.S., Sunitha, N.R. (2019) “Deep learning-based model to fight against Ad click fraud” *ACM Southeast Conference, ACMSE 2019,* Kennesaw State University Kennesaw; United States, Code 147761, [Електронний ресурс]. – Режим доступу:https://dl.acm.org/doi/pdf/10.1145/3299815.3314453?download=true, (Accessed 12 May 2020).

12. Carin M. M. Reep-van den Bergh & Marianne Junger (2018), “Victims of cybercrime in Europe: a review of victim surveys”, *Crime Science*, Volume 7, Issue 1, [Електронний ресурс]. – Режим доступу: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-018-0079-3, (Accessed 12 May 2020).

13. Catalin Cimpanu, (2020), “Gustuff Android banking trojan targets 125+ banking, IM, and cryptocurrency apps”, *Zero Day*, [Електронний ресурс]. – Режим доступу: https://www.zdnet.com/article/gustuff-android-banking-trojan-targets-100-banking-im-and-cryptocurrency-apps/, (Accessed 15 May 2020).

14. Huang, D.Y., Aliapoulios, M.M., Li, V.G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., McCoy, D. (2018), “Tracking Ransomware End-to-end”, *IEEE Symposium on Security and Privacy*, art. no. 8418627, pp. 618-631, ISBN: 978-153864352-5, doi: 10.1109/SP.2018.00047.

15. The official site of Kaspersky antivirus, (2020), “Geografyja rasprostranenyja semejstva Trojan-Banker.AndroidOS.Asacub”, [Online], [Електронний ресурс]. – Режим доступу: https://threats.kaspersky.com/ru/threat/Trojan-Banker.AndroidOS.Asacub/, (Accessed 15 May 2020)

16. Singh, A., Kaur, M. (2019), “Detection Framework for Content-Based Cybercrime in Online Social Networks Using Metaheuristic”, *Arabian Journal for Science and Engineering,* Volume 45, Issue 4, Pages 2705-2719.

17. Rohith, C., Batth, R.S. (2019), “Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War between Nations and its Repercussion”, *International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019*; Amity University Dubai; United Arab Emirates; 11-12 December 2019, Category number CFP19U42-ART; Code 157936, [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/abstract/document/9004236, (Accessed 15 May 2020).

18. The official site of MalwareBytes, (2020), “Emotet”, [Електронний ресурс]. – Режим доступу: https://www.malwarebytes.com/emotet/, (Accessed 15 May 2020).

19. Azeez, S.N., Shivashankaran, T., Gururaj, H.L. (2019), “A research on cyber security awareness based on big data”, *International Journal of Recent Technology and Engineering,* Volume 8, Issue 2 Special Issue 8, August 2019, Pages 1798-1802.

20. The official site of MalwareBytes, (2020), “Trojan.TrickBot”, [Електронний ресурс]. – Режим доступу: https://www.f-secure.com/v-descs/trojan_w32_ursnif.shtml, (Accessed 15 May 2020).

21. Scott Ferguson, (2019), “Ursin banking Trojan variant steals more than Financial Data”, Bank info Security, [Електронний ресурс]. – Режим доступу: https://www.bankinfosecurity.com/ursnif-banking-trojan-variant-steals-more-than-financial-data-a-12165, (Accessed 15 May 2020).

22. Whitty, M.T. (2019) “Predicting susceptibility to cyber-fraud victimhood”, *Journal of Financial Crime,* vol 26, issue 1, [Електронний ресурс]. – Режим доступу: https://www.emerald.com/insight/content/doi/10.1108/JFC-10-2017-0095/full/html (Accessed 12 May 2020)

23. De Arruda, G.F., Costa, L.D.F., Rodrigues, F.A. (2012), “A complex networks approach for data clustering”, *Physica A: Statistical Mechanics and its Applications*, 391 (23), pp. 6174-6183. Cited 14 times, doi: 10.1016/j.physa.2012.07.007.

24. Nir Somech, (2019), “IcedID Banking Trojan Spruces Up Injection Tactics to Add Stealth”, *Security Intelligence*, [Електронний ресурс]. – Режим доступу: https://securityintelligence.com/icedid-banking-trojan-spruces-up-injection-tactics-to-add-stealth/, (Accessed 15 May 2020)

25. Agus, Y.M., Falih, M.D., Satrya, G.B., (2020), “On the possibilities of cybercrime in IoT devices”, *Test Engineering and Management*, Volume 83, Pages 8231-8238.

26. Charlie Ozborn, (2020), “Panda Banker Trojan becomes part of Emotet threat distribution platform”, ZdNet, [Електронний ресурс]. – Режим доступу: https://www.zdnet.com/article/panda-trojan-becomes-part-of-emotet-threat-distribution-platform/,(Access 15 May 2020)

27. Sun Yin, H., Vatrapu, R. (2017), “A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning”, *IEEE International Conference on Big Data, Big Data 2017*, January 2018, pp. 3690-3699, ISBN: 978-153862714-3, doi: 10.1109/BigData.2017.8258365

28. Clauset, A., Newman, M.E.J., Moore, C., (2004), “Finding community structure in very large networks”, *Statistical, Nonlinear, and Soft Matter Physics*, art. no. 066111, pp. 1-6.,doi: 10.1103/PhysRevE.70.066111

References.

1. Goldsmith, D. Grauer, K. and Shmalo, Y., (2020), “Analyzing hack subnetworks in the bitcoin transaction graph”, *Applied Network Science*, vol. 5.

2. Protiviti Inc. (2020), “Executive perspectives on top risks for 2020”, available at: https://www.protiviti.com/CA-en/insights/protiviti-top-risks-survey (Accessed 15 May 2020).

3. Bormann, C. Castellani, A.P. and Shelby, Z. (2012), "CoAP: An application protocol for billions of tiny internet nodes", *IEEE Internet Computing*, art. no. 6159216, pp. 62-67., doi: 10.1109/MIC.2012.29.

4. Pons, P. (2013) "Computing communities in large networks using random walks", *Internet measurement conference*, Barcelona, Spain, pp. 127-140.

5. Nwankwo, W. and Ukaoha, K.C. (2019), "Socio-technical perspectives on cybersecurity: Nigeria's cybercrime legislation in review", *International Journal of Recent Technology and Engineering,* Vol. 8, no. 10, pp. 47-58, available at: https://www.researchgate.net/publication/337033615_Socio-Technical_Perspectives_On_Cybersecurity_Nigeria's_Cybercrime_Legislation_In_Review (Accessed 15 May 2020).

6. Sharma, K. Bhasin, S. and Bharadwaj Nalini, P. (2019), "A worldwide analysis of cyber security and cyber crime using twitter", *International Journal of Engineering and Advanced Technology*, Vol. 8,no. 6 Special Issue 3, pp. 1051-1056, available at: https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13330986S319.pdf, (Accessed 12 May 2020).

7. Insurance Information Institute (2020), "Facts + Statistics: Identity theft and cybercrime", available at: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (Accessed 15 May 2020).

8. Shalaginov, A. Kotsiuba, I. and Iqbal, A. (2019), "Cybercrime Investigations in the Era of Smart Applications: Way Forward Through Big Data", *IEEE International Conference on Big Data*, Los Angeles, United States; 9-12 December 2019, Category number CFP19BGD-ART; Code 157991.

9. NetGuardians (2020), "Digital banking fraud: Best practice for technology-based prevention", available at: https://netguardians.ch/digital-banking-fraud/ (Accessed 15 May 2020).

10. Shishkova, T. (2018), "The rise of mobile banker Asacub", *Kaspersky,* available at: https://securelist.com/the-rise-of-mobile-banker-asacub/87591/ (Accessed 15 May 2020).

11. Thejas, G.S. Boroojeni, K.G. Chandna, K. Bhatia, I. Iyengar, S.S. and Sunitha, N.R. (2019), "Deep learning-based model to fight against Ad click fraud", *ACM Southeast Conference, ACMSE 2019,* Kennesaw State University Kennesaw; United States, Code 147761, available at https://dl.acm.org/doi/pdf/10.1145/3299815.3314453?download=true (Accessed 12 May 2020).

12. Carin, M. M. Reep-van den Bergh and Junger, M. (2018), "Victims of cybercrime in Europe: a review of victim surveys", *Crime Science*, Vol. 7, no. 1, available at: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-018-0079-3, (Accessed 12 May 2020).

13. Cimpanu, C. (2020), "Gustuff Android banking trojan targets 125+ banking, IM, and cryptocurrency apps", *Zero Day*, available at: https://www.zdnet.com/article/gustuff-android-banking-trojan-targets-100-banking-im-and-cryptocurrency-apps/, (Accessed 15 May 2020).

14. Huang, D.Y. Aliapoulios, M.M. Li, V.G. Invernizzi, L. Bursztein, E. McRoberts, K. Levin, J. and McCoy, D. (2018), "Tracking Ransomware End-to-end", *IEEE Symposium on Security and Privacy*, art. no. 8418627, pp. 618-631, ISBN: 978-153864352-5, doi: 10.1109/SP.2018.00047.

15. The official site of Kaspersky antivirus (2020), "Geografyja rasprostranenyja semejstva Trojan-Banker.AndroidOS.Asacub", [Online], available at: https://threats.kaspersky.com/ru/threat/Trojan-Banker.AndroidOS.Asacub/ (Accessed 15 May 2020)

16. Singh, A. and Kaur, M. (2019), "Detection Framework for Content-Based Cybercrime in Online Social Networks Using Metaheuristic", *Arabian Journal for Science and Engineering,* Volume 45, no. 4, pp. 2705-2719.

17. Rohith, C. and Batth, R.S. (2019), "Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War between Nations and its Repercussion", *International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019*; Amity University Dubai, United Arab Emirates, 11-12 December 2019, Category number CFP19U42-ART; Code 157936, available at: https://ieeexplore.ieee.org/abstract/document/9004236, (Accessed 15 May 2020).

18. The official site of MalwareBytes (2020), "Emotet", [Online], available at: https://www.malwarebytes.com/emotet/ (Accessed 15 May 2020).

19. Azeez, S.N. Shivashankaran, T. and Gururaj, H.L. (2019), "A research on cyber security awareness based on big data", *International Journal of Recent Technology and Engineering,* Volume 8, no. 2 Special Issue 8, August 2019, pp. 1798-1802.

20. The official site of MalwareBytes (2020), "Trojan.TrickBot", [Online], available at: https://www.f-secure.com/v-descs/trojan_w32_ursnif.shtml, (Accessed 15 May 2020).

21. Ferguson, S. (2019), "Ursin banking Trojan variant steals more than Financial Data", Bank info Security, [Online], available at: https://www.bankinfosecurity.com/ursnif-banking-trojan-variant-steals-more-than-financial-data-a-12165 (Accessed 15 May 2020).

22. Whitty, M.T. (2019), "Predicting susceptibility to cyber-fraud victimhood", *Journal of Financial Crime,* vol. 26, no. 1, available at: https://www.emerald.com/insight/content/doi/10.1108/JFC-10-2017-0095/full/html (Accessed 12 May 2020)

23. De Arruda, G.F. Costa, L.D.F. and Rodrigues, F.A. (2012), "A complex networks approach for data clustering", *Physica A: Statistical Mechanics and its Applications*, vol.391 (23), pp. 6174-6183, Cited 14 times, doi: 10.1016/j.physa.2012.07.007.

24. Somech, N. (2019), "IcedID Banking Trojan Spruces Up Injection Tactics to Add Stealth", *Security Intelligence*, [Online], available at: https://securityintelligence.com/icedid-banking-trojan-spruces-up-injection-tactics-to-add-stealth/, (Accessed 15 May 2020)

25. Agus, Y.M. Falih, M.D. and Satrya, G.B., (2020), "On the possibilities of cybercrime in IoT devices", *Test Engineering and Management*, Vol. 83, pp. 8231-8238.

26. Ozborn, C. (2020), “Panda Banker Trojan becomes part of Emotet threat distribution platform”, ZdNet, [Online], available at: https://www.zdnet.com/article/panda-trojan-becomes-part-of-emotet-threat-distribution-platform/ (Access 15 May 2020)

27. Sun Yin, H. and Vatrapu, R. (2017), “A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning”, *IEEE International Conference on Big Data, Big Data 2017*, January 2018, pp. 3690-3699, ISBN: 978-153862714-3, doi: 10.1109/BigData.2017.8258365

28. Clauset, A. Newman, M.E.J. and Moore, C., (2004), “Finding community structure in very large networks”, *Statistical, Nonlinear, and Soft Matter Physics*, art. no. 066111, pp. 1-6.,doi: 10.1103/PhysRevE.70.066111

Стаття надійшла до редакції 16.05.2020 р.