DOI: 10.55643/ser.3.45.2022.461

IMPROVEMENT OF COUNTERING ILLEGAL FINANCIAL TRANSACTIONS WITH PAYMENT CARDS

Victoria Bozhenko
PhD in Economics, Associate Professor, Sumy State University, Sumy, Ukraine, email v.bozhenko@uabs.sumdu.edu.ua
ORCID: 0000-0002-9435-0065
(Corresponding author)

Anastasiia Kildei
Student, Sumy State University, Sumy, Ukraine
ORCID: 0000-0002-3439-5456

Hlib Lieonov
Student, Technical University of Hamburg, Germany;
ORCID: 0000-0002-7104-9253

ABSTRACT

The article summarizes the arguments and counter-arguments in the scientific debate on the relationship between cyber fraud and financial crime. The main purpose of the study is to improve the system of counteraction to illegal financial transactions using payment cards. The urgency of solving this scientific problem is due to the fact that increasing online payments, and rising the volume of non-cash payments using bank payment cards creates conditions for various forms of fraud that require legal regulation and identifying possible ways to combat such crimes. The study found that the degree of fraud is directly influenced by factors such as a low level of digital and financial literacy; a lack of a standardized customer authentication system; a large amount of financial and personnel data; relatively low efficiency of the information security control system of banks. According to the analysis of the current state and trends in the financial sector, the following subsystems have been identified that make up the general system of combating fraud with bank payments, such as banking management (functional subsystem), information and communication technology management (technological subsystem), regulatory support legislative subsystem) and increasing the level of digital and financial literacy of consumers of financial services (educational subsystem). The results of the study have practical value for the management of financial institutions to improve the system of combating illegal financial transactions using payment cards, namely the creation of separate bodies for analysis and regulation of fraud in the banking sector, strengthening responsibility for fraud at the legislative level, establishing a single, development of open banking system.

Keywords: fraud, payment instruments, bank cards, financial crimes

JEL Classification: D62, D82, G20, G32, H56

INTRODUCTION

The rapid development of digital technologies and the increase in the density of Internet coverage in the country have provoked an increase in online payments and the growth of using bank payment cards [1]. "Cyber frauds are becoming increasingly sophisticated because banks must keep up with the latest cybersecurity technologies. Any social upheaval, such as earthquakes, war, or country default, is an incentive for intruders to become more active, and therefore, understanding the main methods of cyber fraud and the peculiarities of cyber-attacks in Ukraine is highly relevant, as it allows to respond quickly to the most significant challenges for both banking institutions and, to some extent, for bank customers" [13, p. 19].

The rapid pace of modernization of the banking sector and the emergence of new payment methods have become the basis for the emergence of various forms of fraud that require legal regulation and improvement in the system of combating financial crimes. Losses from fraud in the financial sector are borne by both the payment service provider and the financial consumers.

The main types of attacks on the banking sector are Deepfakes, Zero Trust, phishing, DDoS, brute force, IDOR, XSS vulnerability, SQL injection, malware installation.

Received: 01/07/2022
Accepted: 21/08/2022
Published: 30/09/2022

DOI: 10.55643/ser.3.45.2022.461

According to Merchant Savvy, the losses from fraud with bank payments in the world during 2011-2020 tripled: from 9.84 to 32.39 billion US dollars. According to their forecasts, the volume of losses from fraud with bank payment cards will grow steadily and is expected to reach 40.62 billion US dollars in 2027, which is 25% higher than in 2020 [2]. One of the biggest consequences is the decline in public confidence in financial institutions, which further hinders the use of public money as an investment tool for the development of the national economy.

LITERATURE REVIEW

The scientific works, which study the actual problems of the development of the payment instruments market, including payment cards of banks, show quite serious attention paid by leading scientists to the analysis of modern trends in the role of payment cards in the organization of money circulation and their impact on the course of economic processes.

M. Idzik and K. Sobchak study the development of the non-cash payments market based on a comparative assessment of the use of payment cards in the European Union, paying special attention to the development of payment infrastructure and pointing to the tendency to reduce the number of ATMs due to the introduction of cards with the contactless payment function, as well as the introduction of payments by smartphones [30]. Similarly, S. Gibman, the purpose of his analysis, determined the development of the infrastructure of payment systems, carrying out a comparative assessment of technical and information instruments for the circulation of payment cards and systems such as Apple Pay or applications based on blockchain [31]. L. Kantnerova studies the peculiarities of using payment cards in retail trade, providing trading enterprises with appropriate payment terminals and the impact that this factor has on satisfaction with payment cards and services associated with them [32].

With the development of technology and continuous economic growth, acts of fraud have become much more common in the financial sector. During 2000-2021, the number of scientific publications with the keywords "fraud" and "card", published in journals included in the scientometric database Scopus, is 1791 documents. In particular, O. Caelen from the Worldline Research Center (Lyon, France) has 16 publications, most of which are written in the fields of computer science, engineering, and mathematics. In his work [3] "Detection of credit card fraud: realistic modeling and a new learning strategy" the author believes that the most effective method for analyzing and detecting criminal acts with bank payments is artificial intelligence. On the example of the work of M. Shanmugam etc. [4], it has been proven that money transfers and financial payments are the most popular means of Internet banking in the UK. The authors of this paper noted that the security of financial transactions is the most important factor influencing the speed of implementation of Internet banking in the UK. Y. Li and H. Zhang in [5] propose a technology, the essence of which is to generate one-time card numbers with some secret parameter known only to the cardholder and issuer. According to the study, such a scheme carries less burden on credit card issuers and can be organized in the field of offline and online payments.

In current conditions, the issue of cyber-attacks is quite relevant. It is covered in numerous both general scientific and specialized scientific works, for example, the works Analysis of the consequences of cyber fraud in the banking system of Ukraine (Yarovenko & Boyadzhyan, 2018) [19] or Cybersecurity as an essential component of the national security protection system of European countries (A. Voitsikhovsky, 2018) [15], etc. The legal framework for information and cybersecurity is reflected in the publication of Novytskyi V. (2022) [16]. At the same time, since the article's publication, the National Bank has updated the legal framework for cybersecurity. The monograph of Bakalynskyi (2020) [14] formulated recommendations for building an effective information security system, but, again, without considering global and Ukrainian trends of our time. This problem is typical for other scientists, including Trofymenko O. et al. (2019) [17], A. Ya. Kuznetsova, & N. P. Pohorelenko (2021) [18] since the preparation of the study requires a long time, during which many circumstances can change, especially in the field of banking cybersecurity.

AIMS AND OBJECTIVES

The aim of the article is to develop conceptual foundations for the system of combating fraud with bank payment cards. To achieve the aim, the following objectives are solved in the article:

- the state of the payment card market in Ukraine is analyzed;
- the chronology of cyberattacks on the banking system of Ukraine is summarized;
- subsystems that make up the general system of combating fraud with bank payments are distinguished.

METHODS

The study uses general scientific and empirical techniques and tools of economic science, methods of analysis and synthesis, comparison, summary and grouping. To study the development of the current state of the use of payment cards as an effective means of non-cash payments in Ukraine, statistical methods were used, as well as methods of analysis and observation. The method of summarizing the results was used to formulate conclusions on trends and development of directions for improving the system of counteraction to illegal financial transactions with payment cards.

RESULTS

In Ukraine, the number and volume of non-cash payments using payment cards continue to grow, which is determined, among other things, by the further efforts of the National Bank to digitally transform the financial system. In particular, over the last period, the regulator has taken measures to simplify the issue of payment cards and carry out transactions with their use:

- the possibilities of using businesses of corporate payment cards have been expanded;
- the procedure for obtaining a payment card by an authorized person of an individual – account holder has been simplified;
- the possibilities of carrying out transactions with payment cards with the use of cloud services provided using equipment located on the territory of developed countries have been expanded.

Table 1. Dynamics of the number of payment cards issued by Ukrainian banks by type of information carriers, million units. *(Source: [12, 33])*

Indicators	2017	2018	2019	2020	2021
Total number of issued payment cards in circulation	59.9	59.4	68.9	73.4	89.1
Active payment cards	34.9	36.9	42.2	40.4	46.3
Contactless payment cards	2.7	4.0	8.6	13.2	20.0
Tokenized payment cards	-	-	2.5	3.9	6.7

As can be seen from the data provided in Table 1, the total number of payment cards issued by commercial banks of Ukraine over the past five years has increased by almost 50%: from 60 to 90 million units. And only in the last year, the growth rate was 21.3% compared to the previous period. At the same time, more than half of the issued payment cards (52%) were active payment instruments used by economic agents to carry out expenditure transactions.

The share of non-cash payments using payment cards in Ukraine increased to almost 61% at the end of 2021 from 56% at the beginning of the year. The number of transactions using payment cards issued by commercial banks of Ukraine reached 7817.1 million units, and their amount – UAH 5091.7 billion, which is almost a third (by 30.3% and 28.7%, respectively) more than in 2020 (Table 2).

Table 2. Dynamics of the number and volume of transactions made using payment cards in Ukraine. *(Source: [12, 33])*

Years	Total amount, million pcs.	Non-cash transactions		Cash withdrawal		Total amount, UAH billion	Non-cash transactions		Cash withdrawal	
		million pcs.	%	million pcs.	%		billion UAH	%	billion UAH	%
2017	3091	2311	74.8	780	25.2	2125	835	39.3	1290	60.7
2018	3915	3073	78.5	842	21.5	2876	1297	45.1	1579	54.9
2019	5057	4167	82.4	890	17.6	3576	1798	50.3	1778	49.7
2020	5997	5211	86.9	786	13.1	3958	2209	55.8	1749	44.2
2021	7817.1	7039.9	90.1	777.2	9.9	5091.7	3099.1	60.9	1992.6	39.1

Given in Table. 2 trends indicate the increasing readiness of market entities in Ukraine to use payment cards as a means of payment for goods and services in the process of non-cash payments, and not as a tool for receiving cash at the bank's

DOI: 10.55643/ser.3.45.2022.461

cash desk or ATM. Unlike bank deposits, payment cards demonstrate better liquidity and, consequently, reliability for storing funds, and therefore enjoy a higher level of public confidence. In addition, there is a stable positive trend of growth in the share of non-cash transactions also for the reason that new generations of customers who are more knowledgeable in digital technologies create a corresponding demand for modern banking payment services.

Despite constant audits, control of financial transactions, additional levels of customer base verification, and continuous improvement of information security systems, crime with bank payment cards remains one of the most common crimes in the banking sector. The main factors that determine the banking system's sensitivity to criminal activity are:

- the storage and processing of large amounts of financial and personnel data;
- low level of digital literacy among the population;
- lack of standardized customer verification systems;
- low efficiency of the information security control system of banks;
- non-compliance by the bank's managers with the institution's standards for fraud prevention.

The largest cyberattacks on the banking sector and bank customers in January-August 2022 are shown in Figure 1.

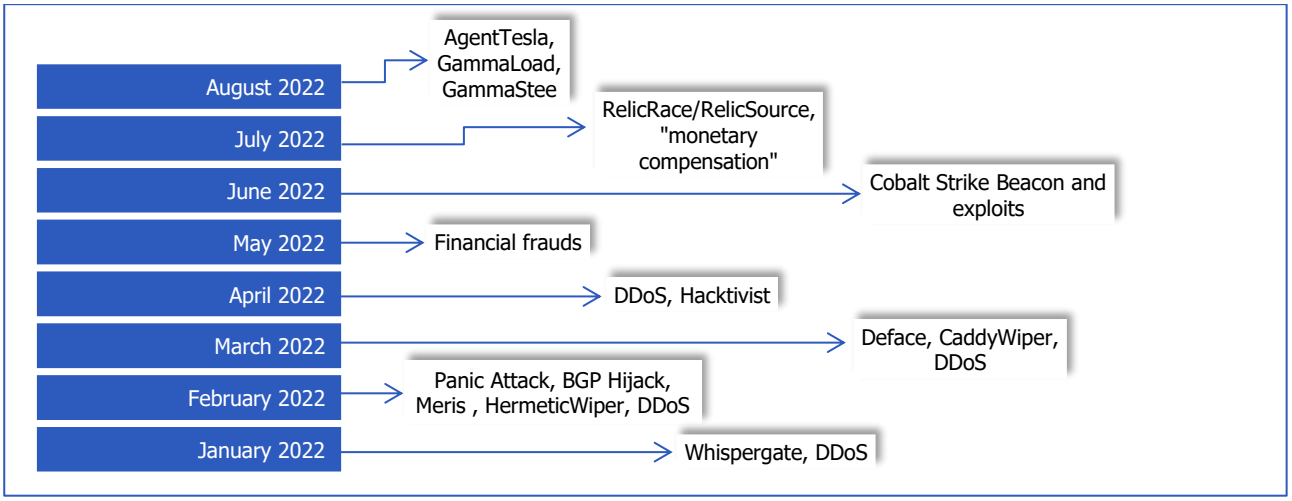

Figure 1. Chronology of cyber-attacks on the banking system of Ukraine in 2022. *(Source: [13, 20-29]*

Fraud with the use of bank payment cards is a global problem that affects not only Ukraine. Thus, according to the European Central Bank, the total volume of transactions in 2019 is 5.16 trillion euros, of which 1.87 billion euros were recognized as fraudulent [6]. In 2019, the volume of fraudulent banking transactions increased by 3.4% compared to 2018. The volume of CNP fraud (cardless transactions) continues to grow, the share of which in 2019 is 80% of the total fraud. Instead, fraud in ATMs and POS terminals was reduced to 5% and 15% of the total cost, respectively.

In the countries of the European Union, the number of fraudulent transactions with bank cards in 2019 grew faster than their corresponding value. In 2019, the average cost of fraudulent transactions decreased by 10% compared to 2018 [7].

According to a survey of top management of financial institutions of Ukraine conducted by specialists of the National Bank of Ukraine, as of November 2021, one of the main sources of risk for the domestic financial sector is fraud and cyber threats (2nd place among the analyzed threats after "corruption, law enforcement and the judiciary "). In November 2021, 16% of respondents rated the factor of "fraud and cyber threats" at a very high level, while in November 2020 this figure was only 3% of respondents [8].

As for Ukraine, the number of payment cards in circulation is growing steadily every year and as of November 2021 is 43.81 million units. During 2011-2021, the average annual growth rate of transactions using electronic means of payment in Ukraine was 22.96%. In 11 months of 2021, the volume of non-cash transactions using payment cards amounted to UAH 2,766 billion, which is 25.22% more than in 12 months [8].

The average amount of one illegal transaction in 2020 averages UAH 1,900, which is 10% less than in 2019. The number of fraudulent actions with payment cards, by contrast, increased by 41% and amounted to 101 thousand units. [8].

Dynamics of the share of losses from fraud with payments by the method of implementation (2019-2020): decreased in the retail network from 0.0066% to 0.0061%; increased in ATMs from 0.0022% to 0.0033%; remained unchanged on the Internet at 0.0061% [9].

Thus, after analyzing the national financial statements, we can conclude that the more contactless, token, and other types of cards are issued - the greater the risk of falling victim to fraud. Currently, most losses are incurred via the Internet, followed by ATMs and retail chains. The average amounts, on the other hand, show a radically different picture: the ATM accounts for UAH 3,646 of the average fraudulent transaction, the Internet for UAH 1,622, and retail chains for UAH 1,984.

Currently, one of the most common types of fraud is social engineering. The essence of the method is to motivate the "victims" to provide their personal data or make a transfer of money to the accounts of fraudsters.

Viking, as one of the methods of fraud with the use of social engineering, is to use methods of communication (phone calls, messages, emails) in retaliation for confidential information. Scammers are usually represented by a bank employee who reports unusual transactions on your account. According to the attacker, the CVV code, PIN code, card number, and/or other conference data must be reported to verify the account.

Usually, this scheme is designed for the elderly due to low awareness. The main incentive to disclose their data is the operator, who puts pressure and emphasizes the urgency of the situation.

These statistics indicate that the issue of fraud with bank payments in Ukraine is acute, as the number and losses from them are growing every year. In the next section, we will consider ways to improve the system of combating illegal actions with payment cards.

An effective fight against payment fraud requires continuous improvement of forms and methods of combating illegal transactions, identifying vulnerabilities in the information security system of the financial institution, as well as the introduction of a set of preventive measures to reduce the number and frequency of fraudulent transactions with bank cards.

Fraud with bank payment cards is an increased public danger, as it damages a wide range of people, which has a destructive effect on the level of confidence in banking services and financial inclusion. Today, crime with the use of electronic means of payment has no borders, and therefore to effectively combat such criminal acts it is necessary to use the recommendations of international agencies and cooperate with international companies. That is why an important role in combating payment fraud is to unite the efforts of financial institutions, as well as regulatory, supervisory, and supervisory authorities [10,11]. With the coordinated and joint activities of the above institutions, the risk of spreading fraud with means of payment can be reduced. Based on this, the system of combating fraud with means of payment should be three-tier, which includes cooperation and interaction of international organizations, government agencies, as well as banking institutions and their customers (Figure 2). Effective ways to combat fraud in the banking sector can be coordinated actions in such areas as banking management (functional subsystem), management of information and communication technologies (technological subsystem), regulatory support (legislative subsystem), and raising the level of digital and financial literacy of consumers of financial services (educational subsystem).

The educational system is to expand knowledge about financial literacy. This subsystem includes not only educational work from banking institutions but also special subjects in educational institutions, and training for children. This direction will allow growing financially aware citizens. For the older generation, it is also proposed to set up information centers where it will be possible to consult a specialist about any operation that may be fraudulent. We offer to disseminate information about measures that can help identify bank fraud.

The legislative subsystem includes the creation of modern regulation of fraudulent banking operations, prosecution of criminally responsible persons, and the provision of appropriate penalties. To implement these proposals, it is necessary to respond quickly and accurately to any changes and "trends" in the types of fraud with bank payments, as well as to actively involve international experts in preventive security.

The functional subsystem is mostly to conduct full monitoring and analysis of all types of payments in terms of systems such as Internet banking, customer banking, and more. The main condition is that the analysis and monitoring include data on all banks to facilitate the further formation of lists of potential fraudsters.

DOI: 10.55643/ser.3.45.2022.461

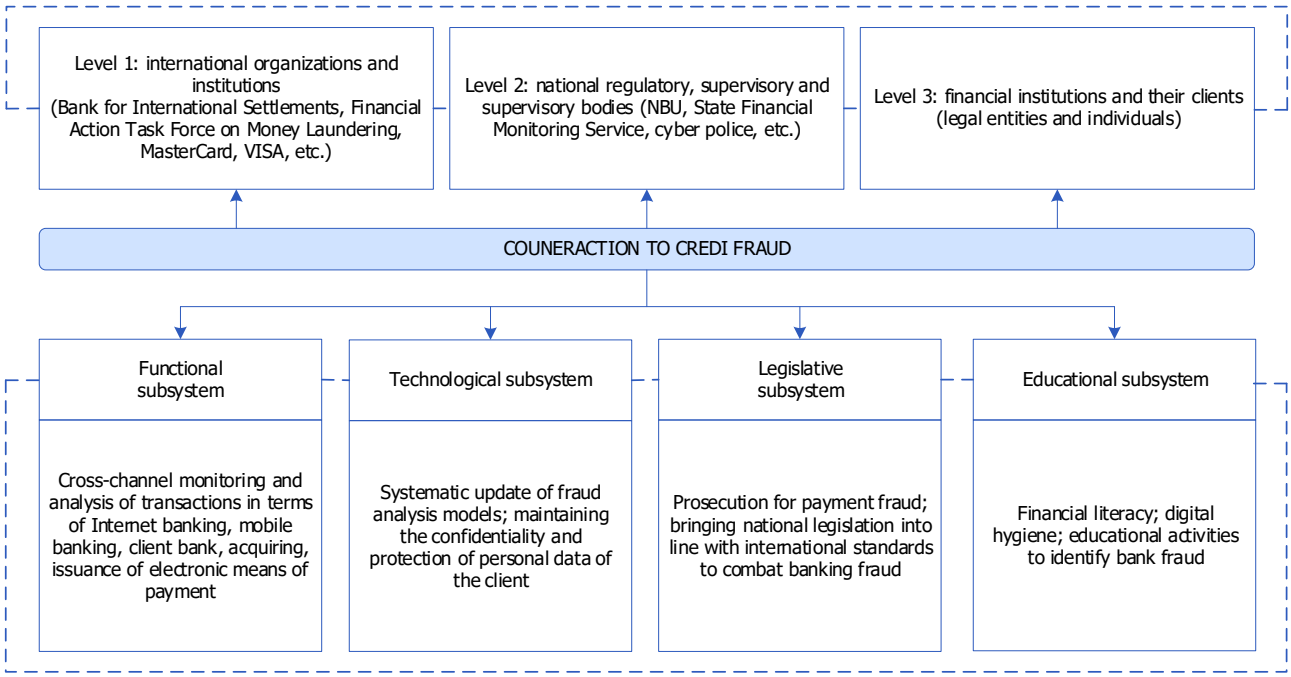

Figure. 2. Key elements of the system of counteraction to fraud with bank payment cards.

The technological subsystem includes the use of the most modern methods for detecting fraud in banking operations. To stimulate scientists, we propose to create material measures to increase interest in this topic to study modern methods of fraud analysis. Also, it is important to constantly maintain the proper level of confidentiality of customers, and their personal data.

DISCUSSION

In the process of dynamic development of the world economy, there are extremely high requirements for availability, safety, speed, convenience and cost of payments and transfers of funds. The inability of traditional paper money to fully meet the needs of consumers arising at the present stage of economic development increases the role of non-cash transactions and payment systems and services.

We agree with scientists Dziubliuk, O., Lutsiv, B., & Chaikovskyi, Y. (2022) who note that "payment cards as a key tool for remote access to bank accounts are the main driver of the development of cashless payment operations and the promotion of the institutional foundations of money circulation in the direction of the increasing growth of its cashless component, which reflects society's demand for reduction in price, acceleration and improvement of payments. Global processes of building economic relations based on digital transformation make this trend irreversible" [12, p. 51].

Despite the huge opportunities provided by the use of payment cards in the process of improving the quality, speed and security of payments, reducing circulation costs and simplifying settlement transactions, further active development of the payment card market is limited to the action of certain deterrents, the presence of which is determined by two key circumstances: on the one hand, the still existing advantages of using cash, which is attractive to a significant proportion of households, On the other hand, there are certain problems that accompany the development of the financial sector in general, and the payment card market itself in particular. One of these problems is cyber fraud with payment cards.

In research Kloba, L., & Kloba, T. (2022), based on the analysis of public information on the chronology of large cyberattacks on the banking sector, a "list of features of cyber threats to banks and their clients was formed, namely: adaptability of the banking sector to the latest cyber threats; strengthening the responsibility of banks before the regulator, including financial responsibility; remote work of bank specialists, which creates an increase in the risk of the human factor; Swedish Malware Update; psychological orientation of cyberattacks" [13, p. 19]. We support the features of cyber threats of banks and their customers listed by these scientists and believe that they should be the subject of further research by scientists.

CONCLUSIONS

Global trends in the development of the financial sector show that the payment card market, which meets the needs to improve the convenience, speed and security of payment transactions, paves the way for the final movement of the banking services mechanism in a new era of the digital economy, and payment cards are the main driver of promoting the institutional foundations of money circulation towards a cashless society.

The payment card market in Ukraine is currently actively developing and has a steady upward trend, but improving the quality of card services, and thus increasing the market largely depends on solving problems associated with the need to introduce new services and forms of services on bank cards, regulating the manifestations of monopoly in the market of payment transactions, active measures for the further development of payment infrastructure, as well as overcoming institutional shortcomings in the development of the financial sector as a whole and developing an active anti-fraud system.

Information insecurity is the most dangerous for banks, therefore, when solving this problem, the bank must take into account the fact that one of the main conditions for the stable functioning of each bank is the exchange of information. That is, the basis of information security should be based on measures to protect the information in the means and networks of its transmission and processing, as well as the creation of an appropriate regulatory framework that would regulate the procedure for accessing, storing and using information from a company, bank, enterprise.

The most common types of intentional threats of today are the following in terms of frequency of manifestation: copying and theft of software; unauthorized data entry; change or destruction of data on magnetic media; sabotage; theft of information; unauthorized use of computer resources; unauthorized use of automated banking systems; unauthorized access to information of a high level of secrecy. The main task of banking information security is to provide conditions for preventing illegal or unfair leakage of commercial information and its use in criminal or illegal actions.

In case of violation of information security of financial institutions, this may lead to actual loss of funds of customers of the banking institution (individuals and legal entities); inability to actively use the free funds of citizens as an investment resource; loss of reputation caused by the disclosure of banking secrecy, personal data, etc; legal claims from affected clients; the need to acquire more sophisticated means of protection to ensure an appropriate level of information security; search for qualified specialists to address current and future gaps in the bank's information security system.

ADDITIONAL INFORMATION

FUNDING

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

REFERENCES

1. Anzhela Kuznetsova, Galyna Azarenkova and Ievgeniia Olefir (2017). Implementation of the "bail-in" mechanism in the banking system of Ukraine. *Banks and Bank Systems, 12*(3), 269-282. https://doi.org/10.21511/bbs.12(3-1).2017.11.
2. Global Payment Fraud Statistics, Trends & Forecasts. Merchant Savvy: веб-сайт. URL: https://www.merchantsavvy.co.uk/payment-fraud-statistics/ (дата звернення 25.01.2022).
3. Dal Pozzolo A., Boracchi G., Caelen O., Alippi C., Bontempi G. Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE Transactions on Neural Networks and Learning Systems. 2017. P. 1-14.
4. Shanmugam M., Wang Y.-Y., Bugshan H., Hajli N. Understanding customerperceptions of internet banking: the case of the UK. Journal of Enterprise Information Management. 2015. Vol. 28. P. 622-636.
5. Li Y. and Zhang X. Securing Credit Card Transactions with One-Time Payment Scheme. Electronic Commerce Research and Applications. 2005. №4 (4) P. 413-426.
6. Seventh report on card fraud. European Central Bank, 2019. URL: https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202110~cac4c418e8.en.pdf (дата звернення 21.01.2022).
7. Opytuvannia pro systemni ryzyky finansovoho sektoru. Natsionalnyi bank Ukrainy. Lystopad 2021 roku. URL: https://bank.gov.ua/admin_uploads/article/Risk_Survey_2021-H2.pdf?v=4

DOI: 10.55643/ser.3.45.2022.461

8. Platezhi ta rozrakhunky. Natsionalnyi bank Ukrainy veb-sait. URL: https://bank.gov.ua/ua/payments

9. Analiz rynku platizhnykh kartok ta shakhraiskykh operatsii z yikh vykorystanniam. URL: https://docs.google.com/presentation/d/1B3jtIWzbAJQngat_QnIMwWcyvHfMnuDv3/edit#slide=id.p5

10. Anzhela Kuznyetsova and Nataliya Pogorelenko (2018). Assessment of the banking system financial stability based on the differential approach. *Banks and Bank Systems, 13*(3), 120-133. https://doi.org/10.21511/bbs.13(3).2018.12.

11. Nafchi A. R., Dastgir, M. Identification and Ranking of Risk Factors Affecting the Probability of Bank Fraud (Case Study, Isfahan Province Resalat Bank): International journal of Business Management. 2019. №4 (4), P. 50–64. URL: https://inlnk.ru/20Qk5d

12. Dziubliuk, O., Lutsiv, B., & Chaikovskyi, Y. (2022). MODERN DEVELOPMENT OF THE PAYMENT CARD MARKET IN THE DIGITAL ECONOMY. *Financial and Credit Activity Problems of Theory and Practice, 6*(47), 51–64. https://doi.org/10.55643/fcaptp.6.47.2022.3894

13. Kloba, L., & Kloba, T. (2022). CYBER THREATS OF THE BANKING SECTOR IN THE CONDITIONS OF THE WAR IN UKRAINE. *Financial and Credit Activity Problems of Theory and Practice, 5*(46), 19–28. https://doi.org/10.55643/fcaptp.5.46.2022.3883

14. Bakalynskyi, O. (2022). Model and methods for determining the design characteristics of information security management systems. Retrieved September 23, 2022, from https://www.researchgate.net/publication/348788054_Model_ta_metodi_viznacenna_proektnih_harakteristik_sistem_upravlinna_informacijnou_bezpekou_Monografia

15. Voytsikhovskyi, A. (2018, January 1). Cyber security as an important component of the national security protection system of European countries. Retrieved September 23, 2022, from https://www.academia.edu/39795468/+

16. Novytskyi, V. (2022). Strategic principles of ensuring information security in modern conditions. Information and law, (1(40), 111–118. Retrieved September 23, 2022, from http://il.ippi.org.ua/article/view/254349 . DOI: https://doi.org/10.37750/2616-6798.2022.1(40).254349

17. Trofymenko, O., Prokop, Y., Loginova, N., & Zadereyko, O. (2022, September 23). Cybersecurity of Ukraine: analysis of the current state. Information Protection, Vol. 21, 3. Retrieved September 23, 2022, from http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y. DOI: https://doi.org/10.18372/24107840/21/13951

18. A. Ya. Kuznetsova, & N. P. Pohorelenko. (2021). MECHANISM OF PROVIDING FINANCIAL STABILITY OF THE BANKING SYSTEM OF UKRAINE. *Financial and Credit Activity Problems of Theory and Practice, 2*(33), 37–47. https://doi.org/10.18371/fcaptp.v2i33.206396ю

19. Yarovenko, A. M., & Boyajian, M. M. (2018, July 18). Analysis of the consequences of cyber fraud in the banking system of Ukraine. http://economyandsociety.in.ua/journals/18_ukr/116.pdf DOI: https://doi.org/10.32782/2524-0072/2018-18-116

20. CERT-UA. (2022, April 28). cert.gov.ua. Research of DDoS attacks that are carried out as a result of the defeat of websites using the malicious JavaScript code BrownFlood. Retrieved September 23, 2022, from https://cert.gov.ua/article/39923

21. CERT-UA. (2022, August 10). cert.gov.ua. UAC-0010 (Armageddon) group cyberattacks: GammaLoad, GammaSteel malware. Retrieved September 23, 2022, from https://cert.gov.ua/article/1229152

22. CERT-UA. (2022, February 18). cert.gov.ua. Information about cyber-attacks on February 15, 2022 Retrieved September 23, 2022, from https://cert.gov.ua/article/37139

23. CERT-UA. (2022, January 26). Fragment of the study of cyber-attacks on 14.01.2022. Retrieved September 23, 2022, from https://cert.gov.ua/article/18101

24. CERT-UA. (2022, July 14). cert.gov.ua. Online fraud with the use of "monetary compensation" theme Retrieved September 23, 2022, from https://cert.gov.ua/article/761668

25. CERT-UA. (2022, June 2). cert.gov.ua. Cyberattack on Ukrainian state organizations using Cobalt Strike Beacon malware and vulnerability exploits CVE-2021-40444 і CVE-2022-30190. Retrieved September 23, 2022, from https://cert.gov.ua/article/40559

26. CERT-UA. (2022, June 20). cert.gov.ua. Cyberattack of UAC-0098 group on critical infrastructure facilities of Ukraine. Retrieved September 23, 2022, from https://cert.gov.ua/article/339662

27. CERT-UA. (2022, May 14). cert.gov.ua. Online fraud using the theme of "financial assistance under the

social program OOH Retrieved September 23, 2022, from https://cert.gov.ua/article/40263

28. CERT-UA. (2022, May 60). cert.gov.ua. Cyberattack of APT28 group with the use of malicious program CredoMap_v2. Retrieved September 23, 2022, from https://cert.gov.ua/article/40102
29. CERT-UA. (2022, September 20). cert.gov.ua. Retrieved September 23, 2022, from https://cert.gov.ua/
30. Idzik, M., Sobczak, K. (2018). Rozwój rynku kart płatniczych w Polsce na tle pozostałych krajów Unii Europejskiej. Wiadomości Statystyczne, No 1 (680), 77-95. http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-22f8669e-85c1-4589-9111-6a1a880ca91d.
31. Giebmann, S. (2018). Money, Credit, and Digital Payment 1971/2014: From the Credit Card to Apple Pay. Administration and Society,No 50(28), 1259–1279. https://doi.org/10.1177/0095399718794169.
32. Kantnerová, L. (2016). Payment Cards. Naše gospodarstvo/Our Economy, No 62(3), 20-28. https://doi.org/10.1515/ngoe-2016-0015
33. National Bank of Ukraine. (2022). Statistics at the National Bank of Ukraine. Retrieved from https://bank.gov.ua/en/

Боженко В., Кільдей А., Лєонов Г.

УДОСКОНАЛЕННЯ СИСТЕМИ ПРОТИДІЇ НЕЛЕГАЛЬНИМ ФІНАНСОВИМ ОПЕРАЦІЯМ ІЗ ПЛАТІЖНИМИ КАРТКАМИ

Стаття узагальнює аргументи та контраргументи в межах наукової дискусії з питання взаємозв'язку між кібершахрайством та фінансовими злочинами. Основною метою проведеного дослідження є вдосконалення системи протидії нелегальним фінансовим операціям із використанням платіжних карток. Актуальність вирішення даної наукової проблеми обумовлена тим, що збільшення розрахунків у мережі Інтернет, нарощення обсягів безготівкових розрахунків із використанням банківських платіжних карток створюють умови для появи різноманітних форм шахрайства, що потребують правового регулювання та визначення можливих шляхів боротьби з такими злочинами. У процесі дослідження було виявлено, що на ступінь шахрайства прямо впливають такі чинники: низький рівень цифрової та фінансової грамотності; відсутність стандартизованої системи аутентифікації клієнтів; великий об'єм даних про фінансове становище, діяльність клієнтів; відносно низька ефективність системи контролю за інформаційною безпекою банків. За результатами аналізу сучасного становища та тенденцій у фінансовому секторі були виокремлені такі підсистеми, що складають загальну систему протидії шахрайству з банківськими платежами, як: управління банківською діяльністю (функціональна підсистема), управління інформаційно-комунікаційними технологіями (технологічна підсистема), нормативно-правове забезпечення (законодавча підсистема) і підвищення рівня цифрової та фінансової грамотності споживачів фінансових послуг (освітня підсистема). Результати дослідження мають практичну цінність для менеджменту фінансових установ для вдосконалення системи протидії нелегальним фінансовим операціям із використанням платіжних карток, а саме: створення окремих органів аналізу та регулювання шахрайства в банківському секторі, посилення відповідальності за скоєння шахрайства на законодавчому рівні, установлення єдиного стандарту системи аутентифікації для клієнтів, розвиток системи відкритого банкінгу.

Ключові слова: шахрайство, платіжні інструменти, банківські картки, фінансові злочини

JEL Класифікація: D62, D82, G20, G32, H56

DOI: 10.55643/ser.3.45.2022.461