Advances in Economics, Business and Management Research, volume 188
Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021)

Ways to Improve Protection Against Cyber Crime in the Banking Sphere

Olha Kovalova [1 * [0000-0003-4555-0172]], Vasyl Kovalov [2 [0000-0001-7172-5832]]

[1] *Donetsk State University of Internal Affairs, Kyiv, Ukraine*
[2] *Donetsk Scientific Recearch Forensic Center of the Ministry of Internal Affairs of Ukraine, Kyiv, Ukraine*
[*] *kovaleva88olga@gmail.com*

ABSTRACT
In today's world, countries have managed to introduce and adapt their basic institutions to the digital economy, operate successfully in the global market and show high results in world rankings, which has a positive impact on various spheres of life, from education to economics. The digitalization of the banking sector has been stimulated by a number of factors, which has led to the need to improve and innovate the banking sector; the spread of the mobile Internet. It should be noted that the rapid development of information technology is constantly creating new types of services, including in the financial sector, as a result of which, criminals have financial or other material benefits in the form of illegally obtained income, which in turn leads to completely new fraudulent online schemes. One of the main factors contributing to cybercrime is the low level of digital literacy of the population regarding personal cybersecurity, especially when using banking products. Some people do not have simple computer skills. Therefore, the priority for our country should be two areas in the fight against cybercrime: actively informing the public about new types of banking services on the Internet and updating legislation in this area to combat crime in cyberspace.

Keywords*: cyberspace, digitalization, banking sector, information technologies, threat, cybercrime.*

1. INTRODUCTION

Today, humanity is experiencing a rapid information revolution involving the formation, development and spread of cross-border global information and telecommunications networks that cover all countries and continents, penetrate every home and simultaneously affect each individual and the vast masses of people. Intensive processes of informatization and intellectualization are taking place in society. If at the beginning of the XXI century few people used mobile communication [1, 2], and the Internet was just gaining strength, today we are on the threshold of interactive television, increasing the speed of information processing, creating various databases. areas of network and cloud systems, smartphones, tablets, intelligent robots. With the advent of the network of information dissemination, in particular, the Internet environment [3] of understanding the place, role, importance of man in the communicative space has undergone appropriate changes.

Today, technological systems are used in science, politics, economics, social structure, increasing the speed of information processing, creating various databases, network and cloud systems, which leads to the formation of global cyberspace. The implementation of computer technology with great potential has led to the computerization of economic and managerial activities, as well as other areas of society, in which the disruption of the normal operation of such equipment can cause huge economic losses. But despite all these positive features of public information, we also have a downside, due to the possibility of committing new crimes by non-traditional means.

2. FORMULATION OF THE PROBLEM

The integrated and large-scale use of information technology based on personal computers, computer networks and computerized communication systems has provided humanity with a new stage of development - the stage of the information society. The impact of information on all spheres of society has led to changes in the world economy, one element of which is the banking system, which ensures the rational use of financial resources and control over their proper accumulation. With the constant changes and the spread

of digitalization, the banking system is undergoing a phase of restructuring and improvement of its mechanisms through the introduction of new devices and technologies in the scope of its activities. New information technologies are helping banks change their relationships with customers and find new ways to make a profit.

Despite all the positive features of digitalization of the banking system, the use of new information technologies and the transfer of public relations to the digital field, you can see the negative consequences associated with the emergence of new types of offenses related to the use of new computer technologies and systems. Accordingly, the fight against these crimes must be in line with modern trends in scientific and technological progress.

3. ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

Cybersecurity is defined as the state of protection of certain objects of the state, in particular banking institutions, from the risk of cyber influence. A large number of works by both domestic and foreign scientists are devoted to the topic of cybersecurity. Questions on the study of the formation of modern cyberspace, the interpretation of the concept of "cybercrime" were engaged in such scientists as: Burova O.Yu., Budakovym M.O., Butuzovym V.M., Halamboiu M.M., Kaliuzhnym R.A., Kamyshyn V.V., Kravtsova M.O., Lytvynov O.M., Maksymenko Yu.Ye., Nizovtsev Yu.Yu., Orlova O.V. Polikhun N.I., Rosynska O.R., Tolubko B., Tropina T.L., Khoroshko V.O., Tsymbaliuk V.S., Cherkun O.M., Yudin O.K. and other. Certain issues concerning the criminal-legal characterization of crimes with the use of information technologies and directions of counteraction to them were considered by such scientists as Azarovym D.S., Aleskerovym V.I., Bilenchukom P.D., Vekhovym V.B., Hlushkovym V.A., Hutorovoiu N.A., Karchevskyi N.V., Mazurovym V.A., Orlovym P.I., Orlovym S.A., Khavroniukom N.I., Yefremovoiu M.A. and others. Research of problematic issues of digital development of banking activity, digital transformation of banking institutions and cyber protection of banking system as Bratkevych P.P., Zymmerman D., KarboValverde S., Kamyshyn V.V., Kliff D., Lytvynov O.M., Manzhai O.V., Nizovtsev Yu.Yu., Parfylo O.A., Puhachevska K.Y., Romaniuk B.V., Rouza D., Rosynska O.R., Tolubko B., Tropina T.L., Khoroshko V.O., Tsymbaliuk V.S., Cherkun O.M. However, researchers focus mainly on individual components of the bank's cybersecurity system. Therefore, the analysis of scientific works shows that despite the significant study, in the context of rapid development and growing role of digital technologies, the issues of democratization of the banking system in the development of modern technologies need further study and analysis.

Working in this direction, researchers have highlighted the problems related to various industries, such as: electronic banking [4]; mobile banking; e-government services [5]; open resources [6]; the ratio of the concepts of "state" and "public" [7]; phishing; electronic resources and services as tools to increase the effectiveness of public policy in various fields.

4. PURPOSE AND TASKS OF THE RESEARCH

The purpose of the article is to form new and develop existing theoretical provisions, as well as methodological tools for combating cybercrime in the banking sector.

To achieve this goal should perform the following tasks:

- to study the transformational changes of the traditional banking sector in the context of digitalization;

- outline the advantages and risks of digitalization of the banking sector;

- analyze the main forms and factors of cyber threats;

- to consider perspective directions on counteraction and prevention of commission of crimes with use of information technologies in the banking sphere.

5. RESEARCH METHODOLOGY

To study the organizational and technical principles, provisions and principles of the introduction of modern means of communication as the main used dialectical method, which allowed to consider the subject of the article in the aggregate and the relationship of its components. In addition, the tasks set to achieve the goal were solved using a set of general scientific and special methods, including formal-logical (analysis, synthesis, deduction, induction, analogy, abstraction), system-structural and comparative law.

6. PRESENTATION OF THE BASIC MATERIAL

In the context of globalization and internationalization of the world there is a new economic system. Modern technology has flooded almost the entire world, which has led to the transformation of many social, economic, political and financial changes [8, 9]. Digital technologies in the form of personal computers and the Internet have already transformed work, education, management, entertainment, leisure, created new market opportunities, leading to significant economic consequences in a wide range of sectors [10].

Improving the development of the banking system leads to the rational use of resources, which gives the state a competitive advantage to participate in the global financial process. Countries that have managed to

introduce and adapt their core institutions to the conditions of the digital economy are successfully operating in the global market and show high results in world rankings. According to the Law of Ukraine "On Banks and Banking", banking - attracting deposits of individuals and legal entities and placing these funds on their own behalf, on their own terms and at their own risk, opening and maintaining bank accounts of individuals and legal entities [10].

The development of modern information technologies in the banking sector has been stimulated by a number of factors: financial crises, which have led to a loss of consumer confidence in the old banking system; raising the standard of living of society, which led to the need to improve and innovate the banking sector; the spread of the mobile Internet. These factors required a review of the banking sector under the new conditions: transparency, trust and organization. Thus, the Internet has significantly expanded the market of banking products and services, including all types of services, including Internet banking. Service in the form of Internet banking allows to expand the customer base, make banking services more efficient and convenient and increase the bank's income. This is a technology that allows you to not visit the bank during banking operations. This type of service includes such new banking products as payment for online store goods, mobile banking, electronic certification, virtual payment cards, electronic balance, "zone 24", POS-terminals in shopping centers and others that have resulted from the development of the World Wide Web. Moreover, the development of financial technologies leads to the formation of financial ecosystems - systems that combine the use of digital technologies of all financial market participants [10].

However, despite a number of improvements in Ukraine, there are still a number of obstacles to the development and digitalisation of the banking sector. One of the key aspects is low cybersecurity and high levels of fraud in online banking and online services. The diversity of telecommunication resources is a fertile field for the emergence of new sophisticated methods of criminal activity [11]. In such crimes, computer devices or the information stored in them are directly the objects of criminal encroachment or have become a means of committing a crime. This leads to a decrease in customer confidence in new channels and banking platforms in general.

As world practice shows, fraudsters usually use the mechanisms of the main banking operations: credit, deposit and settlement and payment, thereby undermining the foundations of the financial institution. Tarasenko VP notes that financial data is one of the most popular objects of attack, the use of which is aimed at making money by intruders. Crimes in settlement and payment transactions have the highest share in the structure of banking crime and are characterized by a high level of material damage caused to banks. Crimes committed in the banking system or with its use can be considered one of the most dangerous economic crimes, as their negative impact is reflected not only on the bank itself, but also on many other economic entities and the financial system as a whole [12]. Because of this, banking institutions have always been the target of cyber attacks at all levels of the IT infrastructure.

According to UN experts, the term "cybercrime" covers any crime that can be committed through a computer system or network, and therefore none of them is protected from fraud in the field of Internet services. [13]. The concept of cybercrime, however, as well as cybersecurity, is not currently disclosed by the norms of the Convention on Cybercrime of 23.11.2001, which was ratified by Ukraine in 2005, which is probably due to the fact that online banking is directly in Ukraine and online services have entered the daily lives of most citizens relatively recently.

In Ukraine, cybercrime, the criminal law provides and enshrines in a separate Chapter XVI of the Criminal Code of Ukraine, as socially dangerous acts "Crimes in the use of computers, systems and computer networks and telecommunications networks" [14]. But the Criminal Code of Ukraine does not reveal the full essence of the concept of "cybercrime", it contains only general, to some extent outdated, information. Thus, the concept of "cybercrime" was absent in Ukrainian legislation until the adoption of the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" in 2017, in which the legislator discloses the concept of "cybercrime" as a socially dangerous crime in cyberspace and / or use, liability for which is provided by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine [15]. In the Constitution of Ukraine, the concept of "fight against cybercrime" is absent, but in Art. 17 of the Constitution states that ensuring information security of Ukraine is the most important function of the state and the business of the entire Ukrainian people, which, in some ways, is a conflict, because the state does not have sufficient tools to ensure cybersecurity. [16].

Globally, there is a wide range of cybercrimes, including crimes committed for financial gain, crimes involving the use of information contained in a computer, and crimes against the confidentiality, integrity and accessibility of computer systems. In turn, according to current legislation, information is any information and / or data that can be stored on physical media or displayed electronically [17]. More and more personal, corporate and government information is stored on cloud technologies and remote hosting, computing operations are transferred from personal systems to computing clusters, to virtual servers, to cloud technologies.

According to the National Bank of Ukraine, the most common types of cybercrime in the banking system of Ukraine are:

1. *ATM fraud: skimming* - theft of card data using a special reading device; use of "white plastic" for "copying" (forgery) of a payment card and further withdrawal of cash at ATMs;

2. *Fraud in trade and service networks:* "cloning" of payment card details with the use of technical means; transactions without authorization for an amount less than the established limit;

3. *Fraud in the online space:* forgery of payment card data; making transactions using stolen payment card data; writing software for theft of payment card details (interception of traffic, creation of fake WEB-sites, distribution of Trojans and viruses).

4. *Internet fraud: phishing* - sending an e-mail similar to the address of a well-known brand with a request to log in to a third-party resource, as if to pass a survey on the quality of this brand, for which you will be transferred to the card, but you will need to provide information about card number, validity period and CVV-code. It is through phishing that a person's credit card fraud occurs; SMS greetings about winning in draws in which you did not participate; creation of "financial pyramids" on the Internet; fraud in the sale of goods over the Internet or at online auctions (ie the sale of non-existent goods) [18].

It should be noted that the rapid development of information technology is constantly generating new types of services, including in the financial sector [18], as a result of which, criminals, there are financial or other material benefits in the form of illegally obtained income. First of all, it is about the use of information and communication systems and computer technology for access to private property of legal entities and individuals and further actions to manage or dispose of this property. In particular, access to funds of clients of banking institutions has become the most widespread among cybercrimes today. In modern conditions it is necessary to use a set of software and hardware that would ensure a high level of infrastructure protection while maintaining sufficient process efficiency. To prevent attacks, social engineering methods are effective - it is regularly instructing all employees of the company to work safely on the Internet and informing them about existing types of threats [18].

One of the main factors contributing to the commission of cybercrime is the low level of digital literacy of the population regarding personal cybersecurity, especially when using banking products. Some people do not have simple computer skills. The solution to this problem can be facilitated by the creation of certain online platforms, courses or programs for the education of both the younger generation and the provision of basic skills in the use of information technology by the elderly. Considering foreign experience, we can say that in many leading countries of the world have already formed national cyber security systems.

For example, the UK has set up the Microsoft Cyber Defense Operations Center (CDOC), a 24-hour cybersecurity and defense center with leading security experts and data scientists who protect, detect and respond to threats to Microsoft's cloud infrastructure, products and devices. as well as internal resources. To help British citizens master the skills of use, was to create a program Microsoft digital skills. This program provides everyone with basic skills on the Internet [19].

In the United States, models of preventive activities are used: public institutions, individual safety and environmental impact. In Canada, citizen participation in crime prevention is widely used, reducing the fear of criminals, maintaining a sense of personal security and mastering certain user skills. The German police have introduced targeted preventive work with the public, focused on self-defense, which is carried out through free consultations of the population on how to use technical means to protect property from criminals, not to become a victim of crime.

Ukraine is also in the process of forming a cyber security system. To combat cybercrime in Ukraine, special organizational structures have been established, namely: the Government Commission for Information and Analytical Support of Executive Bodies, the Interdepartmental Committee for the Protection of Intellectual Property Rights, the Interdepartmental Working Group for Development and Approval of the Concept of Legalization of Software Products and combating their illegal use. In 2011, the Department for Combating Cybercrime of the Ministry of Internal Affairs of Ukraine was opened, and the relevant territorial units began to be established in early 2012. On November 5, 2015, a new Cyberpolice was established as a structural unit of the National Police. The main purpose of the cyber police was to reform and develop units of the Ministry of Internal Affairs of Ukraine, which will ensure the training and operation of highly qualified specialists in expert, operational and investigative police units involved in combating cybercrime [13].

Establishing the fact and circumstances of the crime is usually carried out by obtaining operational information. The terms "computer intelligence", "virtual intelligence", "analytical intelligence", "analytical intelligence via the Internet", "computer monitoring", "cyber intelligence", etc. are used to describe such activities.

Computer intelligence (Internet intelligence) - operational and investigative measures, which consists in the purposeful search and retrieval of information from computer systems and networks, access to which is not

limited to their owner, owner or administrator or not related to overcoming the logical protection carried out by employees of operational and operational-technical units in order to identify information of a criminogenic and criminal nature [20]. *Virtual intelligence* is a set of measures for obtaining, processing and analysis of intelligence information in cybernetic (telecommunication, virtual) space with the help of various types of software and mathematical influence. *Analytical intelligence* by means of the Internet is a complex of information technologies for systematic finding of information in open sources. Recently, specialized computer intelligence programs have been used to carry out computer intelligence. their specific functions of intelligence programs compared to other search and analytical programs, allow you to expand the search area, reduce search time, identify latent connections, increase the value of the information obtained [21].

The essence of computer intelligence is to extract: 1) computer information that is processed, stored and transmitted in information systems; 2) data and information on the characteristics (parameters) of software, hardware and software-hardware complexes used in information systems; 3) data and information on methods, methods and mechanisms of information protection used in information systems; 4) personal information about users of information systems [20].

The following tools and methods are used in cyber intelligence in the investigation of crimes: analysis of open sources of information, social engineering, withdrawal of information from transport telecommunications networks and electronic information systems, obtaining and analyzing information held by telecommunications operators and providers about communication , subscriber, provision of telecommunication services, including receipt of services, their duration, content, transmission routes, etc. [21].

Therefore, given the above facts about the pros and cons of digitalization of the banking sector, the emergence of new threats with the use of information technology, especially when criminals have financial or other material benefits in the form of illegally obtained income, there is a need to take certain measures:

- it is necessary to check the connection with the bank's server;

- it is worth using licensed versions of banking product programs;

- after the end of the Internet, you need to close the browser windows with the banking product;

- no need to store login and password information or any other banking information;

- no one can tell your login and password;

- it is necessary to regularly monitor account statements (for timely detection of unauthorized or erroneous debiting of accounts).

7. CONCLUSIONS

Thus, the prevention of cybercrime today not only remains very important, but also continues to attract more and more attention of scientists and practitioners, as information technology is used in almost all spheres of human life and society. Given the above, we can say that cybersecurity is a top priority in the banking sector around the world. The paper noted both the positive and negative aspects of the digital development of the banking sector. Measures have been proposed, the implementation of which will increase the efficiency of the bank's cybersecurity and the efficiency of the banking business. An effective fight against cybercrime requires a system of measures and the implementation of appropriate public policy in this area. The new laws alone are not able to counter the growth of IT crime. Today, important positions on combating cybercrime in Ukraine include increasing the digital literacy of the population, the introduction of the obligation of operators, providers to store electronic data to ensure their integrity and indisputability, to provide at the legislative level for modern information technology in relevant information and criminal procedure legislation.

REFERENCES

[1] Md Mostafizur Rahman Komol, Amit Kumer Podder, Abdullah Arafat and Tanzim Nabeed (2019), “Remote Sensing Global Ranged Door Lock Security System via Mobile Communication”, *International Journal of Wireless and Microwave Technologies*, vol. 9, no. 5, pp. 25-37, DOI: 10.5815/ijwmt.2019.05.03

[2] Kuboye Bamidele Moses (2014), “Mobile Communication Evolution”, *IJMECS*, vol. 6, no. 1, pp. 25-33, DOI: 10.5815/ijmecs.2014.01.03

[3] Rasim Alguliyev and Sabira Ojagverdieva (2019), “Conceptual Model of National Intellectucal System for Children Safety in Internet Environment”, *International Journal of Computer Network and Information Security*, vol. 11, no. 3, pp. 40-47, DOI: 10.5815/ijcnis.2019.03.06

[4] Mugdha, Y. (2020), “Development of conceptual framework for internet banking customer satisfaction index”, *International Journal of Electronic Banking*, vol. 2, no. 1, DOI: 10.1504/IJEBANK.2020.105417

[5] Venkatesh, V. Thong, J. Y. L. Chan, F. K. and Hu, P. J. H. (2016), “Managing citizens’ uncertainty in e-government services: the mediating and moderating roles of transparency and trust”, *Information Systems Research*,

vol. 27 (1), pp. 87–111, DOI: 10.1287/isre.2015.0612

[6] Shevchenko, V.E. (2019), "Open data services in Ukraine", *Aktualni pytannia masovoi komunikatsii*, vol. 26, pp. 41–53, DOI: 10.17721/2312-5160.2019.26.41-53

[7] Durman, M.O. (2020), "The ratio of the concepts of "state" and "public" in the field of regulatory policy: the actualization of the conceptual and terminological apparatus", *Naukovyi visnyk: derzhavne upravlinnia*, vol. 2 (4), pp. 135–149, DOI: 10.32689/2618-0065-2020-2(4)-135-148

[8] Tkachenko, Volodymyr Kwilinski, Aleksy Korystin, Oleksandr Svyrydiuk, Natalia and Tkachenko, Iryna (2019), "Assessment of information technologies influence on financial security of economy", *Journal of security and sustainability issues*, march, vol. 8, no. 3, pp. 375-385, DOI: 10.9770/jssi.2019.8.3(7)

[9] Kovalchuk, T.I. Korystin, O.Y. and Sviridyuk, N.P. (2019), "Hybrid threats in the civil security sector in Ukraine", *Problems of Legality*, vol. 147, pp. 163-175, DOI: 10.21564/2414-990x.147.180550

[10] Savchenko, M. and Negolyuk, Yu. (2021), "Democratization of the banking system under conditions of digital technologies development", *Galician economic journal*, vol. 68, no 1, pp. 103-111, DOI: 10.33108/galicianvisnyk_tntu2021.01.103

[11] Korshenko, Vadym (2017), "Forensic telecommunication examination as a source of evidence during the investigation of cybercrimes", *National Law Journal*, pp. 192-194, available at: http://dspace.univd.edu.ua/xmlui/handle/123456789/3783?locale-attribute=en

[12] Tarasenko, V.P. (2017), "Some cybercrimes in the banking sector and ways to prevent them", *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: materialy Vseukrainskoi naukovo-praktychnoi konferentsii*, pp. 139-141.

[13] Bukhtiarova, A.H. and Hushcha, A.V. (2019), "Countering cybercrime in the banking sector", *Pryazovskyi ekonomichnyi visnyk*, vol 3, pp. 355-361.

[14] "Criminal codex of Ukraine" (2001), № 2341-III, *Baza danykh «Zakonodavstvo Ukrainy»*, *Verkhovna Rada Ukrainy*, available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text

[15] "On the basic principles of cybersecurity in Ukraine" (2017), *Baza danykh «Zakonodavstvo Ukrainy»*, *Verkhovna Rada Ukrainy*, available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text

[16] "Constitution of Ukraine № 254k/96-VR" (1996), *Vidomosti Verkhovnoi Rady Ukrainy*, st. 141, available at: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

[17] "About information: Law of Ukraine" (1992), no 2657-XII, *Vidomosti Verkhovna Rada Ukrainy*, available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text

[18] Mosiichuk, Ye.V. (2019), "Cybersecurity in the field of Internet banking", *materialy Vseukr. nauk.-prakt. konf*, pp. 59-60.

[19] "Supporting the UK in fighting cyber-crime" (2019), available at: https://cloudblogs.microsoft.com/industry-blog/en-gb/cross-industry/2019/11/07/supporting-uk-fighting-cyber-crime/

[20] Kozytska, O.H. (2020), "Cyber intelligence as the newest direction of operative-search activity", *Naukovyi protses ta naukovi pidkhody: metodyka ta realizatsiia doslidzhen*, pp. 107-108.

[21] Baranenko, R.V. (2020), "Use of computer intelligence by units of the National Police of Ukraine", *V Mizhnarodna naukovo-praktychna konferentsiia "Modern scientific and technical methods of management information flow and their influence on the development of society"*, 24-25 liutoho 2020 r., Frankfurt na Maini, Nimechchyna, pp. 85-86.