BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10, Sumy, 40022, Ukraine

www.businessperspectives.org

Received on: 5th of March, 2019
Accepted on: 25th of March, 2019

Olena Kofanova, Ph.D. in Juridical Sciences, National Academy of Internal Affairs, Ukraine.

Yuliia Tereshchenko, Ph.D. in Juridical Sciences, National Academy of Internal Affairs, Ukraine.

Roman Kutsyi, Ph.D. in Juridical Sciences, National Academy of Internal Affairs, Ukraine.

Nadiia Morhun, Ph.D. in Juridical Sciences, National Academy of Internal Affairs, Ukraine.

Oleg Gushchyn, Ph.D. in Juridical Sciences, Kyiv National University named after Taras Shevchenko, Ukraine.

Olena Kofanova (Ukraine), **Yuliia Tereshchenko** (Ukraine), **Roman Kutsyi** (Ukraine), **Nadiia Morhun** (Ukraine), **Oleg Gushchyn** (Ukraine)

ACTUAL SITUATION OF COMPUTER CRIME IN THE CREDIT AND FINANCIAL SPHERE OF UKRAINE (MODERN ASPECTS)

Abstract

The purpose of the article is to study computer crimes in the credit and financial sphere based on elements of forensic characteristics of crimes and analysis of the ways of their commission. The relevance of the study is due to the rapid increase in the number of computer crimes in the credit and financial sphere and the low level of their disclosure. The research was conducted using the method of system analysis and synthesis of information obtained from criminal proceedings, as well as reports from the Ministry of Internal Affairs of Ukraine and the National Police of Ukraine, from 2014 to 2018. The most actual motives and methods of committing computer crimes in the financial sphere have been analyzed and it has been established that during the period of Ukraine's independence, the level of economic crimes has increased by almost 300%. The increase in the number of crimes contributes to the distrust of the injured party to the law enforcement agencies, savings of funds of financial institutions on cyber security, low level of information security of the financial sphere of Ukraine, lack of clear coordination between the relevant departments, which are responsible for the investigation of these crimes. The necessity of conducting separate investigative actions at the initial stage of the investigation has been justified in order to facilitate the rapid identification of the suspect, causing material damage and, in general, the investigation process.

Keywords economic crime, forensic characteristics, unlawful act, cybercrime, criminal investigation

JEL Classification G21, G23, K13, K14

INTRODUCTION

In the present context of socio-economic development of Ukraine, computer crime has become a reality of social life.

Understanding the causes of its occurrence and development requires an analysis of emerging crises and has begun to influence the social, economic and legal development of society.

Information has become the living base of modern society, the subject and product of its activities. In other words, information becomes a product of public (informational) relations related to the production, transmission, accumulation and use of information in its various forms: scientific and technical documentation, software, databases, database management systems, and others.

In this regard, the new information technologies gave impetus not only to the progress of society, but also stimulated the emergence and development of information crimes. Since 1991, according to the Interpol classification, information crimes are divided into: QA – Unauthorized

http://dx.doi.org/10.21511/bbs.14(1).2019.15

access and interception; QD – Changing computer data; QF – Computer fraud; QR – Illegal copying; QS – Computer sabotage; QZ – Other computer crimes. These criminal offenses have been most widely distributed in various sectors of the economy and management, including in manufacturing, banking and consumer services.

1. THEORETICAL BASIS

The new Criminal Code of Ukraine (2001) includes a separate section (section XVI – "Crimes in the area of the use of electronic machines (computers, systems and computer networks"), entirely devoted to the classification and establishment of liability for the commission of computer crimes, which contains three direct rules – Articles 361-363. There are four rules in other sections that have an indirect relation to computer crimes. In the following articles, an electronic computer, its system and a computer network are defined as the object of a crime. In addition, there is another fundamentally new crime subject to Articles 361 to 363, computer information.

Computer crimes (Sergeev, 2005; Skakun, 2018) or cybercrime (Chekotovskaya, 2013; Ramadani, et al., 2018) include a set of crimes provided by the criminal law that encroach on information infrastructure, information, as well as in relation to other objects in cyberspace or using its capabilities. Among all spheres of public life, the most vulnerable is the financial and credit sphere, especially in the sphere of international economic relations.

Forensic characteristics of computer crimes differ from the already known forensic science of criminal encroachment with a certain specificity. There is the view that in the first place, it must include forensic evidence of the offender's identity (Bilenchuk & Kotlyarevsky, 1997), the motives and purpose of his criminal behavior, typical means, the objects and place of the offense, as well as the victim and the traces of the crime.

The fact of the emergence of computer crime in society (Bilenchuk & Kotlyarevsky, 1997; Andreev, Pak, & Horst, 2001) is associated with the emergence of so-called "hackers" (from the English "hacker") – IT specialists who are engaged in the search for illegal means of obtaining unauthorized access to computer facilities and data along with their unauthorized use with a mercenary purpose.

In the process of analyzing the materials of criminal proceedings about computer crimes, it was established that the age of the offender is determined within the limits of 24-45 years: the age of 33% of offenders did not exceed 20 years, 13% were older than 40 years and 54% were 20-40 years old. Men form the majority in this category (83%), but the number of women is rapidly increasing due to the professional orientation of some specialties and professions (Figure 1).

In the professional-classification plan, the circle of "computer" criminals is very broad. All of them can be divided into two main groups, based on the classification mark of the category of access to computer facilities:

Source: Materials of criminal proceedings.

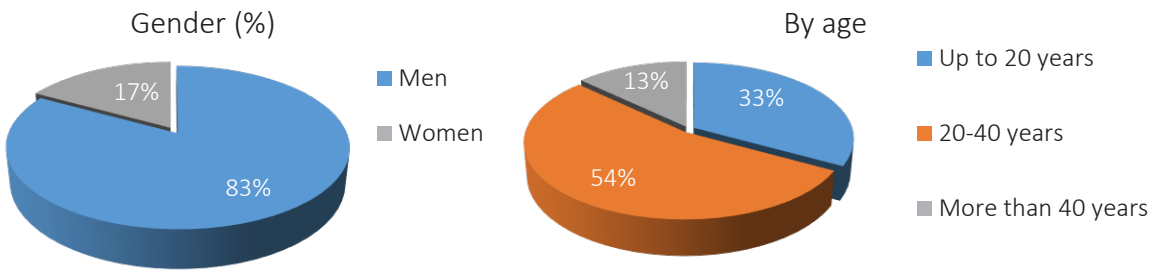

Figure 1. Information about the identity of the offender by age and gender

Source: Materials of criminal proceedings.

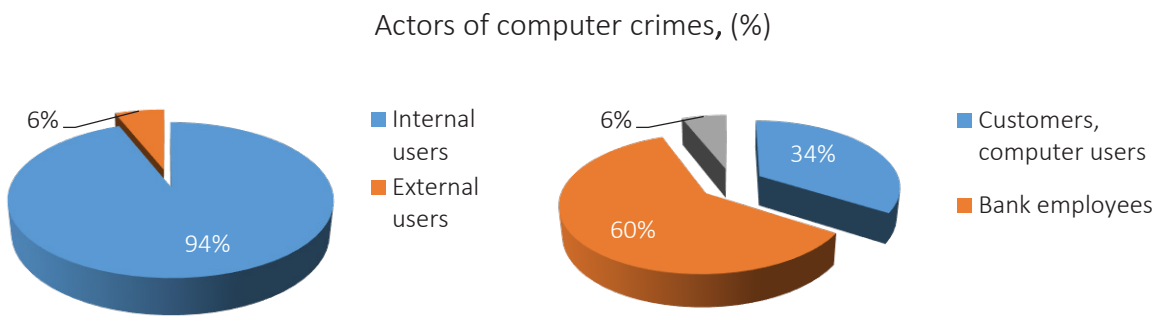

Figure 2. Information about the actors of computer crimes

- internal users;
- external users, where the user (the consumer) is the subject who refers to the information system or the intermediary to obtain the information he needs and uses.

There are two types of users: registered (sanctioned) and unregistered (unauthorized, illegal). According to many experts, the main danger in terms of committing computer crimes comes from internal users (Donaldson, 2016): they commit 94% of crimes, while external users only 6%, 34% account for customers – users of computer systems, and 60% – bank employees (Figure 2).

Such crimes can be divided into three groups based on the functional category of access to computer facilities.

The first group includes offenders who committed computer-based crimes using software. In part, they include computer operators, accountants, cashiers, database administrators and data banks, programmer operators (system and application), software engineers, and others.

The second group includes those who committed computer crimes based on the use of computer hardware: communication operators, terminal equipment engineers, computer auditing specialists and others.

The third group includes persons who have committed computer crimes based on indirect access to computer facilities. There are those who handle organizational issues: computer system management, operator management, database management or data banks, management work on software, managers, and others.

Criminals from outside users, as practice shows, are individuals who are well informed about the activities of the victim. Their circle is very wide, so they can be systematized and classified: it can be any person, even an ordinary person. For example, a representative of an organization engaged in service, repair, software development of computer facilities on a contractual basis, representatives of various supervisory and governing bodies or organizations, clients or hackers.

Consider the motive and purpose of committing computer crimes, which are very important in formulating the forensic nature of the crimes of this case category. The motive and purpose of the committed crimes are directly related to the socio-psychological and forensic characteristics of the offender's personality. Summarizing the information about the most common motive and purpose of committing computer crimes, it should be noted that they belong to the most important components of the forensic characteristics of the crime. Consequently, the motive and purpose of the crimes included in the group of subjective factors that influence the choice of means and methods for achieving purpose, determine the nature of the main actions of the offender, and, accordingly, the content of the method of committing a crime, which represents a complex of voluntary actions of a person and the basic forensic description of any criminal offense.

The motive and purpose in some cases are necessary signs of the subjective side of intentional crimes (for example, a motivated motive for

http://dx.doi.org/10.21511/bbs.14(1).2019.15

abuse of power or office, the purpose of theft of funds in the unauthorized access to data, etc.). For most intentional crimes, the motive and purpose are not necessary elements of the subjective side and, accordingly, not part of the criminal and legal characteristics. Incidentally, in all cases, when investigating a particular crime, the motive and purpose must be clarified. It is important not only for the court to establish a just punishment for the committed but also to facilitate the full disclosure of the crime. Information on the most common grounds and purpose of committing computer crimes is used when introducing versions in relation to the subject and the subjective side, as well as when organizing a criminal prosecution. For example, investigative practice shows that the purpose of damage and destruction of physical carriers of machine information in some cases conceals the theft of material assets or money, when physical carriers of machine information have been damaged or destroyed. Verification of versions about their total or partial destruction in order to conceal theft could lead to the criminals.

2. RESULTS

According to the research results of multiple studies on this issue, one can note the following (Figures 1-4).

The structure of forensic characteristics of computer crimes is equally influenced by the generalization of information on the victim's side. Forensically meaningful information allows for a broader characterization of the perpetrator's identity, motives for committing a crime, and thus helps to to identify more accurately the circle of people who need to look for the perpetrator and search for the most important evidence (Svoboda, Kofanov, & Mihalchuk, 2018).

In particular, the identification and analysis of forensic evidence of the victim's side and its behavior (before, during and after the crime) provides an opportunity to understand deeply many circumstances of the crime, especially pointing the motives of the offender's conduct, his general (typical)

Source: Materials of criminal proceedings.

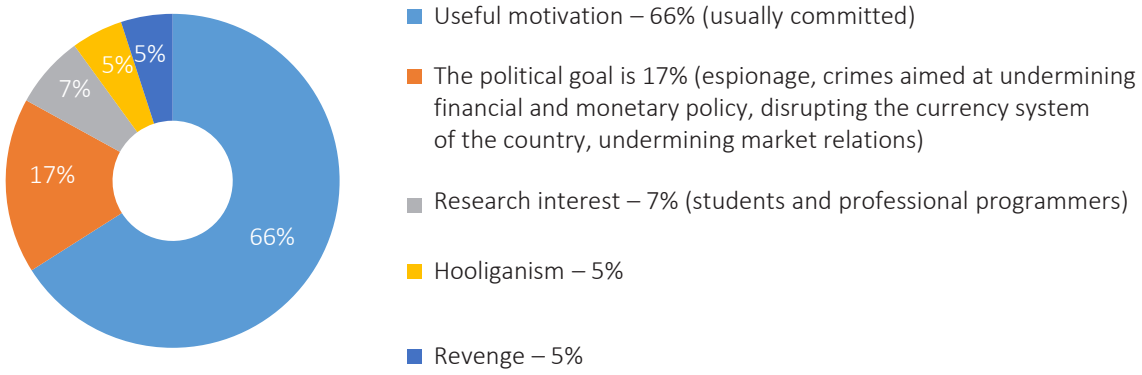

Figure 3. Information about the motives for committing computer crimes

Source: Materials of criminal proceedings.

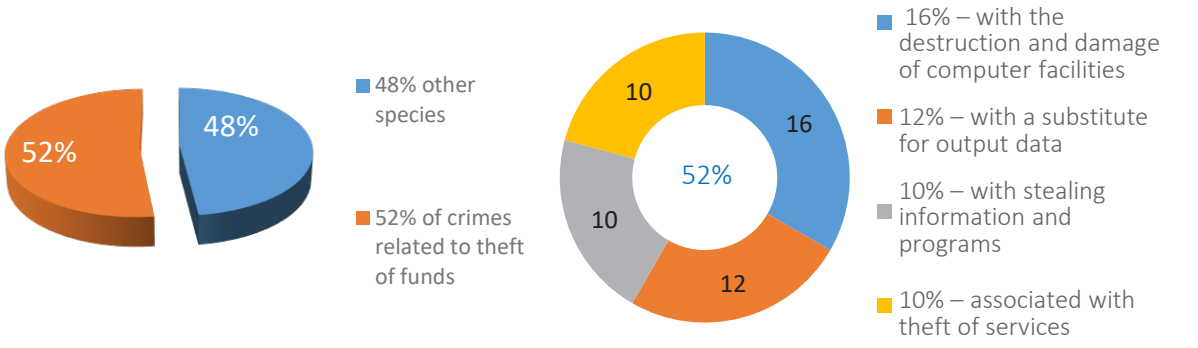

Figure 4. Information about the method of committing crimes related to theft of funds

Source: Materials of criminal proceedings.

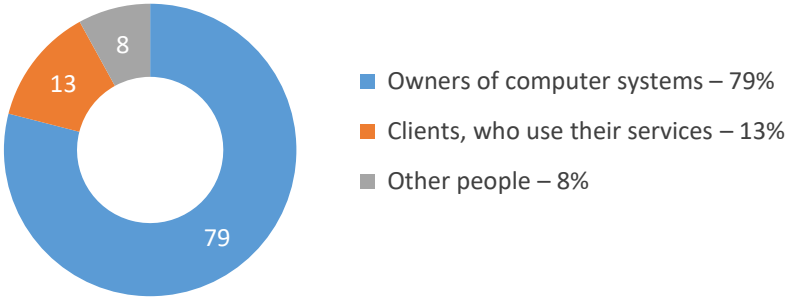

Figure 5. Information about the victim's side of computer crimes

and individual characteristics. This is due to the fact that it is common that there is a certain relationship between the offender and the victim, that makes the criminals not to choose objects of their criminal encroachment accidentally (Figure 5). Especially it is difficult to identify and explore this connection at the beginning of the investigation.

Notable is the fact that the victim of the first group is the owner of the system, reports (if at all) to the law enforcement authorities about an event of a computer crime. And they make up the bulk and, accordingly, the greater number and the very factors of committing such crimes, because this can explain the high level of computer crime latency. In this case, registered computer crimes are as in Figure 6.

Allocate factors influencing the decision by the injured party (Muzyka-Stefanchuk, Huberska, & Yamnenko, 2017) to ask the police for the fact of a computer crime committed against them:

- incompetence of law enforcement in defining the fact of committing a computer crime, of its disclosure and investigation;
- the risk of undermining its own authority in business circles and, as a result, the loss of a significant number of customers. This circumstance characterizes especially banks engaged in a wide automatization of production processes;
- inevitable disclosure of the organization's security system in the course of a judicial investigation;
- identifying the reasons for committing a crime in the course of investigating a computer crime may call into question the professional competence of certain officials, which eventually will lead to negative consequences;
- legal and legislative illiteracy of officials in the issues of this category.

Source: Materials of criminal proceedings.

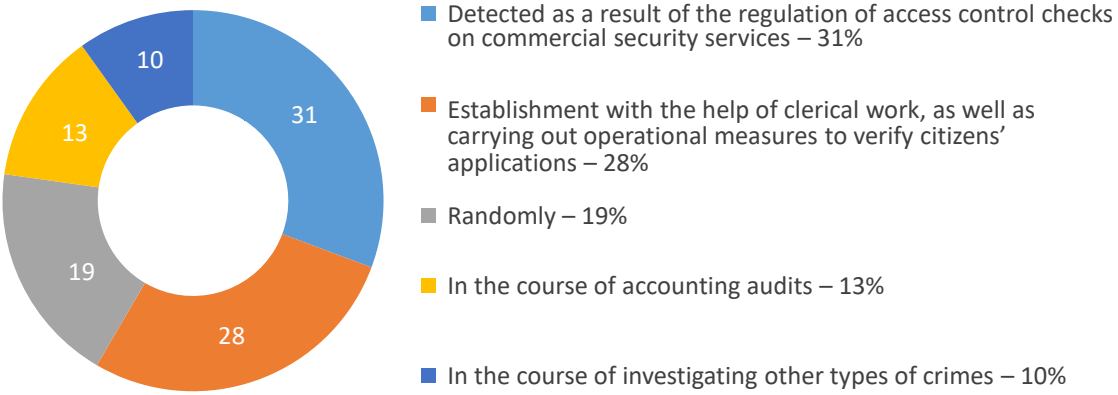

Figure 6. Ways of detecting the fact of committing computer crimes

http://dx.doi.org/10.21511/bbs.14(1).2019.15

2.1. Ways of committing computer crimes in the credit and financial sphere

Economic crime is an unlawful activity that covers various abuses of economic power that violates the order of economic management, causes significant economic damage to the interests of the state, private entrepreneurial activity or groups of citizens, is committed continuously and under the cover of the manager's legal economic activity in order to obtain a profit for both physical and legal persons (Skakun, 2018).

The most acceptable classification of economic crimes is made by the German criminologist Kaiser (1979).

1. Offenses against the banking and shareholder exchange system; credit system; insurance systems and free competition, including abuse of trust and apparent bankruptcy, as well as copyright and labeling rights.

2. Evasion of taxes; fraudulent subsidies; extortion.

3. Bribes.

4. Violation of the legislation on labor protection; crimes against consumers, the environment.

5. Fraud and speculation.

Significant increase in the effectiveness of combating economic crime can only be achieved through a deep economic reform, improvement of legislation that ensures the functioning of a healthy market environment, and the creation of an appropriate legislative framework for law enforcement agencies.

Issues relating to the analysis of crime in general, and economic crime, in particular, are complex and multifaceted. They have not only a great theoretical but also above all practical significance, since it is status of the state's economy that defines all other aspects of society's life, where the future destiny of Ukraine is solved, the foundation of its real sovereignty and international authority is laid. So, when determining the role of the economy in society, one can confidently say that it always "rules the ball".

However, the criminological situation in Ukraine (especially in the sphere of economy) has considerably deteriorated in recent years, which complicates the implementation of fundamental economic reforms of market type, increases social tension in society, creates additional difficulties in the process of developing an independent and sovereign rule of law state.

According to statistics provided by the Ministry of Internal Affairs of Ukraine, economic crime in 1992 amounted to 36,860 crimes, whereas in 2018 it already accounts for 109,825 crimes, which is a 297.5% increase in the number of crimes in comparison with 1992 (Reports from the Ministry of Internal Affairs of Ukraine, 1992, 2018).

There are significant changes in the types of most common crimes in the overall structure of crime in the economy, which to some extent really reflect the trends towards activating criminals. Thus, in 2018, as compared to 2014, crimes in the field of computer systems increased by 3.5 times. At the same time, there is a significant reduction (almost double) of the crimes committed in the budget sphere and those connected with the use of budgetary funds (by almost a third) (Reports from the National Police of Ukraine, 2014–2018).

In the priority areas of the economy (in the credit and financial sector, foreign economic activity, fuel and energy complex, etc.) during 2014–2018, 140 thousand crimes were revealed. In 2018, 2.3 times more than in 2014, criminal proceedings for crimes, losses of which amount to more than USD 3 million. In just five years, such proceedings have been violated by almost 3,000 (Reports from the National Police of Ukraine, 2014–2018).

During the 2014–2018 period, about 17 thousand crimes were revealed in the financial and credit sphere, of which about 5,5 thousand – in banks. On average, the share of crimes committed directly in banks in Ukraine was one-third. In 2018, 30% more than in 2014, criminal proceedings for crimes, losses of which amount to more than 300 thousand UAH was violated. Altogether, over a total of five years, such proceedings have been

violated by almost 2.5 thousand (Reports of the National Police of Ukraine, 2014–2018).

The analysis of international experience of law enforcement units in fighting against economic crime, the substantiated analytical forecast of possible offenses in banking give an opportunity to examine in detail the criminological processes which take place in the main link of the financial and credit system.

In accordance with the technology, structure, circle of participants and methods of committing, such crimes can be divided into those, which are committing directly in the banks, and which are committing in the field of the enterprise, using the institutions of the banking system. Fraud with the use of payment cards and their requisites and fraud with the use of remote banking services (the system "client-bank") are the most widespread crimes in the banking sector. The average value of such crimes in the European Union countries is 0.06-0.08%, in Ukraine, the number of such crimes reached 0.045% of all transactions with payment cards (Chekotovskaya, 2013).

According to the technology of committing such crimes, as well as the structure and the circle of participants of these unlawful acts, their methods can be divided into those carried out directly in the banks, and those that are carried out in the sphere of the enterprise, using the institutions of the banking system. The range of methods for the theft carried out directly in the banks is quite wide – from the appropriation of monetary deposits from accounts of polar depositors who have not made a testamentary order or have no successors to simple appropriation, which is often considered as "temporary borrowing" by cashiers and other materially responsible and the officials of the money entrusted to them and the withdrawal of money from collector's bags by their disguised misappropriation of collectors. However, the listed methods are easy to execute, and the amount of damages is not dangerous. They were known earlier and therefore do not need any detail. The most widespread and socially dangerous is the category of abuses associated with the formation, "laundering" and the illegal use of false money.

The method of committing these abuses is divided into those that are carried out by using:

- payment orders accompanied by false credit memos;
- unsecured limited checkbooks;
- unsecured check books in combination with a credit or debit note;
- letter of credit;
- bills of exchange.

It should be noted that experts in the field of computer systems and some bank managers attribute the reliability of electronic banking networks with the means of their external protection, that is, with the encryption of input into the computer system itself and its levels of information, depending on the admission of a group users. The range of operating personnel who will have access to a wide range of information on banking technology will be large. And this, first and foremost, is a wide circle of people who have various disadvantages. Therefore, the system for protecting electronic networks, which is based only on the management of inputs to various types of information, is ineffective. In order to make a relatively reliable system for protecting banking electronic networks, along with the old, we need fundamentally new approaches. Such a program should be based on the technology of bank document circulation and peculiarities of committing a crime using one form of settlement and credit operations (Thompson, 2018).

DISCUSSION AND CONCLUSION

The research of the whole complex of theoretical and practical problems connected with the peculiarities of investigating crimes committed in the credit and financial sphere of Ukraine using modern information technologies makes it possible to formulate the following conclusions, suggestions and recommendations:

http://dx.doi.org/10.21511/bbs.14(1).2019.15

1. As practice shows, computer crime, as a rule, is based on the territories where the state has not created appropriate conditions for ensuring counteraction to crime, that is, in states with limited capabilities to counter new threats. Thus, the openness of global information networks enables criminals to choose a jurisdiction that is consistent with their criminal ends. International experts believe that most transnational criminal gangs and organizations are in transition and transition economies. So, states with a sufficient level of information technology development and a low ability to deal with crimes in this area become shelters for transnational crime.

2. There is currently a fundamental need to develop expert knowledge of computer crime, to effectively distribute information between relevant departments, to create special units at the national level, to create interagency and international target groups.

3. The results of the analysis of investigative practices conducted show that such investigative actions (such as investigation of the place of the event, search and extraction, interrogation, appointment of examinations) are the most specific, typical and significant for the investigation of computer crimes in the banking system, especially on the initial stage of pre-trial investigation. The urgency of conducting these investigative actions and organizational measures is due to the fact that they are aimed at establishing the crime, its method of execution, the identification of typical traces, the establishment of eyewitnesses, the establishment of offenders and other circumstances that ultimately contribute to the successful investigation of the criminal offenses, fair punishment of guilty and compensation of damages caused to the injured party.

REFERENCES

1. Agres, O., Sodoma, R., & Sadura, O. (2017). Realities and prospects of Ukraine banking system. *Financial and credit activity: problems of theory and practice, 2*(22), 17-23. https://doi.org/10.18371/fcaptp.v2i23.121032
2. Andreev, B., Pak, P., & Horst, V. (2001). *Investigation of crimes in the field of computer information.* Moscow, Russia: Yurlitinform.
3. Andrushko, P. (2000). Problems of criminal responsibility for interference with the work of automated systems. *Legal, normative and metrological provision of the information security system in automated systems of Ukraine,* 50-53.
4. Bilenchuk, P. D. (2003). Взаємодія правоохоронних органів України та країн світу при розслідуванні електронних високотехнологічних транснаціональних злочинів [Vzayemodiia pravookhoronnykh orhaniv Ukrainy ta krain svitu pry rozsliduvanni elektronnykh vysokotekhnolohichnykh transnatsionalnykh zlochyniv]. In P. D. Bilenchuk, L. V. Borisova, & E. K. Paniotov (Eds.), *Pravo i Bezpeka* (Vol. 1, pp. 54-59). Rertrieved from http://nbuv.gov.ua/UJRN/Pib_2003_2_1_15
5. Bilenchuk, P. D., & Kotlyarevsky, O. I. (Eds.) (1997). *Портрет комп'ютерного злочинця: підручник [Portret kompiuternoho zlochyntsia: pidruchnyk]* (48 p.). Kyiv, Ukraine.
6. Bilenchuk, P. D., Dinnik, O. G., Lyuty, I. O., & Skorokhod, O. V. (Eds.) (1999). *Банківське право: українське та європейське: навч. посіб. [Bankivske pravo: ukrainske ta yevropeiske: navch. posib.]* (398 p.). Kyiv, Ukraine: Atika.
7. Chekotovskaya, O. (2013). *Legal regulation of cybercrime*. Center for Judicial Studies.
8. Cherniavsky, S. S. (Ed.) (2003). *Злочини у сфері банківського кредитування (проблеми розслідування та попередження)*: *Навч. посіб.* [*Zlochyny u sferi bankivskoho kredytuvannia (problemy rozsliduvannia ta poperedzhennia): Navch. posib.*] (264 p.). Kyiv: Yurinkom Inter.
9. Donaldson, D. (2016). *Vulnerability of Financial Institutions to Cyber Crime*. Presented. Information Security, CISSP, CISM.
10. Golubev, V. O. (2003). *Інформаційна безпека: проблеми боротьби з кіберзлочинами*: *Монографія [Informatsiina bezpeka: problemy borotby z kiberzlochynamy: Monohrafiia]* (250 p.). Zaporizhzhia: HU "ZIDMU".
11. Hlushchenko, O. (2017). Sustainable development of Ukraine: opportunities and threats. *Financial and credit activity: problems of theory and practice, 2*(23), 372-378. https://doi.org/10.18371/fcaptp.v2i23.121904
12. Kaiser, G. (1979). Criminology. Introduction to the basics.
13. Muzyka-Stefanchuk, O. A., Huberska, N. L., & Yamnenko, T. M. (2017). To understanding behavior of subjects of financial relations. *Financial and credit activity: problems of theory and practice, 22*(1), 315-320. https://doi.org/10.18371/fcaptp.v1i22.110045

14. National Fraud Center (NFC). (2000). *The Growing Global Threat of Economic and Cyber Crime.* Retrieved from https://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf

15. Ramadani, S., Siahaan, A. P. U., Sutrisno, Ritonga, S., Amelia, W. R., Dalimunthe, H., & Munthe, R. (2018). Impact of Cybercrime on Technological and Financial Developments. *International journal for innovative research in multidisciplinary field, 4*(10), 341-344. Retrieved from https://www.researchgate.net/publication/329001306_Impact_of_Cybercrime_on_Technological_and_Financial_Developments

16. Sergeev, V. V. (2005). Computer crimes in the banking sector. *Banking, 2,* 27-28.

17. Skakun, T. O. (2018). Economic crimes: intrinsic features and forensic analysis of their commission. *Efficient economy, 3.* Retrieved from http://www.economy.nayka.com.ua/pdf/3_2018/155.pdf

18. Svoboda, Y. Yu., Kofanov, A. V., & Mihalchuk, T. V. (2018). *Участь спеціаліста-криміналіста під час проведення окремих слідчих (розшукових) дій: підручник [Uchast spetsialista-kryminalista pid chas provedennia okremykh slidchykh (rozshukovykh) dii: pidruchnyk].* Kyiv, Ukraine.

19. Thompson, Ch. (2018). *Cyber crime in financial services: the big picture.* Accenture Finance & Risk Blogs. Retrieved from https://financeandriskblog.accenture.com/cyber-risk/cyber-crime-in-financial-services-the-big-picture

20. Tsimbalyuk, V. S. (2001). Латентність комп'ютерної злочинності [Latentnist kompiuternoii zlochynnosti]. In *Боротьба з організованою злочинністю і корупцією (теорія і практика) [Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)]* (pp. 178-182).

21. Tsimbalyuk, V. S. (2002). Criminological aspects of the commission of offenses in the sphere of international economic relations with the use of information computer technologies. *Collection of scientific works of the Kharkiv Center for the Detection of Organized Crime in conjunction with the American University of Washington, 6,* 234-260.

22. Vurtuzayev, M. S., & Yurchenko, O. M. (Eds.) (2001). *Захист інформації в комп›ютерних системах від несанкціонованого доступу: навчальний посібник [Zakhyst informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu: navchalnyi posibnyk]* (321 p.). Kyiv, Ukraine: European University.

http://dx.doi.org/10.21511/bbs.14(1).2019.15