"Peculiarities of cybercrime investigation in the banking sector of Ukraine: review and analysis"

AUTHORS	Sergij S. Vitvitskiy https://orcid.org/0000-0002-4884-1883
	Oleksandr N. Kurakin https://orcid.org/0000-0002-0274-6530
	Pavlo S. Pokataev https://orcid.org/0000-0003-3806-2197
	Oleksii M. Skriabin https://orcid.org/0000-0002-8915-5943
	Dmytro B. Sanakoiev https://orcid.org/0000-0002-6783-3168

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
38	2	0

Sergij S. Vitvitskiy, Associate Professor, Doctor of Law, Rector of Donetsk Law Institute of the Ministry of Internal Affairs of Ukraine, Ukraine.

Oleksandr N. Kurakin, Associate Professor, Doctor of Law, Deputy Director for Educational and Research Activities of the Kryvyi Rih Educational and Scientific Institute of the Ministry of Internal Affairs of Ukraine, Ukraine.

Pavlo S. Pokataev, Professor, Doctor of Science in Public Administration, Doctor of Law, First Vice-Rector, Classical Private University, Ukraine.

Oleksii M. Skriabin, Associate Professor, Doctor of Law, Associate Professor of Criminal Law, Procedure and Criminology Department, Classical Private University, Ukraine (Corresponding author).

Dmytro B. Sanakoiev, Associate Professor, Ph.D., Head of Financial and Strategic Investigations Department, Faculty of Training for Strategic Investigations Units, Dnipropetrovsk State University of Internal Affairs, Ukraine.

Sergij S. Vitvitskiy (Ukraine), **Oleksandr N. Kurakin** (Ukraine), **Pavlo S. Pokataev** (Ukraine), **Oleksii M. Skriabin** (Ukraine), **Dmytro B. Sanakoiev** (Ukraine)

PECULIARITIES OF CYBERCRIME INVESTIGATION IN THE BANKING SECTOR OF UKRAINE: REVIEW AND ANALYSIS

Abstract

The rapid growth in the number of cybercrimes committed in the banking sector requires the creation of an effective system for preventing such crimes and ensuring the cybersecurity of the state. The constant updating of means and methods for cybercrime commission necessitates the identification of effective measures to combat them. The paper uses a survey method to study the theoretical experience and practical measures to prevent cybercrime in the banking sector to identify effective ways to combat crime in the virtual space of Ukraine. The paper analyzes the experience of the world's leading countries concerning cybercrime prevention, deals with measures to improve the level of cybersecurity of national and international cyberspace. It is concluded that the current state of cybersecurity in Ukraine does not meet contemporary requirements and needs initiating effective measures and coordinated cooperation between private and public sectors in order to effectively combat cybercrime, in particular: enshrining the classification of cybercrimes in the regulatory legal acts of Ukraine; introduction of the concept of "banking criminal law" in the scientific and legal sphere; creation of Ukrainian cyber forces, whose activities will be aimed at preventing and combating crimes committed in cyberspace.

INTRODUCTION

Criminal activity, which every year acquires new forms, methods and technologies for committing crime, is an integral part of public life. Cybercrimes are quite common today in Ukraine and around the world. Virtual crimes are becoming widespread in the banking sector. The number of crimes committed by obtaining access to bank card codes and illegal seizure of funds from accounts is growing every year. The spread of virtual forms of crime is associated primarily with the rapid development of technology, increased role of information in public life, and the ability to commit crimes remotely. Cybercrime is particularly attractive because of the ability to hide or destroy its traces.

Anti-cybercrime activities occupy a special place in the law enforcement agencies activities, due to the latent nature of such criminal offenses and the constant updating of their commission mechanism. The process of investigating these crimes is complicated by the difficulty of detecting and recording traces of crimes in the virtual space. The ability to remotely destroy the traces of crime allows cybercriminals to minimize the amount of crime evidence. The issue of investigating virtual crimes in the banking sector is caused by the specifics of their commission, which requires specialized knowledge of law enforcement officers. It is also noteworthy that cybercrime is interna-

tional in its nature, so there is a need for law enforcement officers to cooperate at the international level to minimize the level of virtual crime in the banking sector. This situation determines the significance of the theoretical study of the banking sector cybercrime investigating process in order to develop measures contributing to the increase of cybersecurity both at the national and international level.

The study aims to analyze and systematize theoretical experience and practical measures to combat cybercrime in the banking sector in order to identify promising ways to combat crimes in the cyberspace of Ukraine.

1. LITERATURE REVIEW

One of the problems that persists in society for a long time is that users of information systems "believe without a reasonable basis in the absence of cyberattacks, using the information space without being aware of the limitations and threats to system security" (Sindhu et al, 2012). Many scientific works by domestic and foreign scientists study cybercrime detection, cessation and investigation, which is due to the novelty and rapid growth of crimes committed in the virtual area.

With the increasing number of Internet users, the following risk factors increase: society's dependence on information technology, followed by the vulnerability to various types of information encroachments; the possibility of using the network to commit crimes, and the potentiality to become a victim of using information technology for criminal purposes is also growing. At the same time, committing a crime does not require much effort and expense – it is enough to have a computer, software and information network connection. You don't even need to have profound technical knowledge: There are special forums where you can buy software for committing crimes, stolen credit card numbers and users' credentials, and use services, which can help you commit electronic embezzlements and computer systems attacks (Ben-Itzhak, 2008).

In a broad sense, cybercrime is classified based on its role in the legal relationship between the personal computer and the Internet, so it is possible to distinguish crimes against a computer or the Internet or crimes committed using a computer or the Internet (Marbeth-Kubicki, 2010).

Among foreign scholars, these issues were studied by Brenner, who investigated criminal threats from cyberspace (2006). In studying cybercrime,

Brenner (2006) identifies the following three categories:

1) crimes in which a computer is the purpose of the crime;

2) crimes in which a computer is used as a means of committing a crime; and

3) crimes in which a computer plays a minor role in the crime commission.

The German Criminal Code introduces the concept of computer fraud, which implies an act that causes property damage through the formation (installation) of incorrect computer programs, the use of incorrect or incomplete data, unauthorized use of data and other illegal influence on electronic information processing, committed for the purpose of obtaining property benefits (both personal and in favor of third parties) (Odenthal, 2009).

In German jurisprudence there are, for example, the following essential elements of cybercrime:

1) crimes committed with the help of statements;

2) invasion of personal privacy;

3) fraud and computer fraud;

4) software and hardware attacks;

5) documents forgery using a computer;

6) other computer crimes (Hilgendorf & Valerius, 2012).

Another interesting classification of cybercrime, suggested by German criminal law researchers, is the following division of cyberspace crimes:

1) fraud with goods purchased at online auctions or online stores;

2) credit card fraud, including at ATMs;

3) new methods of account fraud and money laundering, such as the creation of lodgment companies;

4) advertising fraud using the most typical fraudulent schemes with address books;

5) fraud in the field of fair competition, in particular, aimed at granting a competitive advantage illegally;

6) click fraud, using online advertising (or "sponsorship lists") of services, such as "one click" insurance (Janke, 2008).

The most common crimes in cyberspace are embezzlements committed by deception, which are distinguished according to the following types: payment fraud (payment cards embezzlement); skimming (crimes with the use of ATMs for commission a fraud); malicious payment software (embezzlement through the development and use of malicious software programs); social engineering (illegal obtaining of information for personal gain); phishing (gaining access to confidential personal data by sending e-mails); e-commerce fraud (embezzlement related to the vulnerability of payment systems of online stores, platforms for booking air tickets, car rental and others); prepayment fraud (promise to provide services or deliver goods after prepayment) (Jahankhani et al., 2015).

Aikov et al. (1999) study the guidelines for combating cybercrime. According to Stein (2004), the peculiarity of crimes in cyberspace is that the characteristic of the Internet in terms of jurisdictional policy is to blur the line between domestic and international information transmission.

An important remark within the framework of the issues being studied is to distinguish a concept of the banking criminal law. Thus, legal practitioners in European countries, including the Italian Republic (Giovanni Paolo) and Germany (Steele, 2020), appeal to the concept of "banking criminal law", understanding this definition as a set of criminal offenses committed in the banking sector.

It should be noted that there is a need for further study of cybercrime investigation in the banking sector due to the rapid development of technology, new forms and methods of committing crimes in cyberspace, as well as the spread of crimes in the banking sector. In 2017, a study was undertaken on world's countries ranking concerning the highest level of security. The top ten countries include Singapore (one of the leading countries, according to this report), Malaysia, Oman, Estonia, Mauritania, Australia, Georgia, France and Canada. Equatorial Guinea was recognized as the worst country in terms of implementing the main provisions of the Global Program (Miles, 2017). Thus, according to the results of a global study of economic crimes and fraud conducted in 2018, cybercrime is among the top five crimes in the economic sphere. Compared to 2016, the level of cybercrime increased from 24% to 31% (according to PwC research). Moreover, according to a report presented by Accenture Security, by 2030 the total loss from cybercrime can amount to about USD 90 trillion (Bissel et al., 2017).

Kroes, the European Commissioner for New Technologies Implementation, reasonably stated in her speech at the World Economic Forum in Davos in 2013 that the most serious mistake was to misinterpret cybersecurity as a purely technical task, as the state should be the main subject for its provision. Therefore, the strategic goal is to increase the cybersecurity effectiveness at all government levels (Kroes, 2013).

Among Ukrainian authors who have studied the criminal law and criminalistics aspects of cybercrimes, the peculiarities of their investigation in the banking sector, it is important to note Burbelo, who studied the peculiarities of the forensic foundations of combating cybercrime (Burbelo, 2013); Douschi, who studied the legal and organizational aspects of cybersecurity in Ukraine (Douschi, 2018); Pushkarenko, whose scientific research is devoted to the study of cybercrime in terms of the shadow economy (Pushkarenko, 2006); and Sen, who revealed the features of foreign experience in the cybercrime investigation (Sen, 2014).

It should be noted that in modern society, the largest number of cybercrimes occurs in the financial and banking sectors. Thus, Nekrasov (2016) notes that cybercrime in the financial and banking sector, fraud using payment cards and their details, theft of funds from bank accounts, "money laundering", seizure of confidential computer information about customers, etc. have recently become the most widespread types of crimes.

It should be noted that there are much more cybercrimes committed in the banking sector than it is officially reported. Thus, Bukhtiarova and Hushcha (2019) note that the reason is that many of the cyberattacks are unsuccessful, and the identified gaps in the e-banking system are quickly restored. Dissemination of information about cybercrime attempts can affect the level of customer confidence in a banking institution. As a result, the bank's customers may start withdrawing their bank deposits from banks on a massive scale, which will constitute a severe problem for banks due to a sharp increase in liquidity risk, so it is difficult to estimate the true cybercrime level.

Nowadays in Ukraine, as noted by Leonov and Seriohin (2019), methodological materials are introduced in special expert institutions to provide research of computer media used also for methodological support for studying software products as a means of committing computer crimes. Recommended methods of computer information research and technology for monitoring the activity of the software under investigation can be applied to identify traces of the software function implementation. Establishing and evaluating a set of traces allows one to reproduce, i.e., to model the actions of a computer crime and identify the trace object (program) as a means of crime in solving a diagnostic problem.

Analyzing the Criminal Procedure Code of Ukraine, Rohatiuk (2015) notes that the supervisory activities of prosecutors have been transformed into procedural guidance, which involves direct management of any crime investigation, including cybercrime. With the prosecutor's signature, the investigator's decision-making is agreed at all major stages of the investigation, starting with the covert investigative (search) actions and ending with the indictment. He determines the direction of the investigation, participates in certain investigative (search) actions, and then supports the state prosecution in court.

It is the availability of relevant information technology knowledge and skills that enables the prosecutor to provide effective procedural guidance of cybercrime investigation by investigating officers, gather appropriate evidence and eliminate procedural shortcomings during the investigation.

According to Ismailov and Shaievska (2016), the following factors are the main reasons for the spread of cybercrime:

- firstly, this area of criminal activity is extremely profitable and is on a par with illegal areas of activity such as drug pushing, arms traffic and human trafficking;

- secondly, financial institutions hide most of the facts of cyberattacks on their institutions from law enforcement agencies, taking care of their reputation among customers;

- thirdly, in case of insignificant financial losses, financial institutions do not even conduct internal investigations, taking into account that human, financial and other costs of such conduct exceed the losses;

- fourthly, crimes are committed in a virtual environment if they are very latent.

According to Markov (2015), the specific characteristics of cybercrime are the following:

- the need for widespread use of special knowledge in detecting and recording crime traces in the electronic form;

- organization and transboundariness (broad interregional and international ties);

- high latency caused by the reluctance of the private sector to report such crimes due to distrust of the potential capabilities of law enforcement agencies and unwillingness to acknowledge the weaknesses of their security systems;

- the high level of technical support of criminals.

The investigation of cybercrime in the banking sector has many specific features, as indicated by Mukhin (1999):

- a number of traditional elements of certain criminalistics methods are uninformative or uninformative in relation to the category of computer crimes and the structure of its individual elements; these include the peculiarities of using public assistance in solving crimes, the peculiarities of the victim's personality;

- a special role is played by information on the peculiarities of using special knowledge in solving and investigating crimes under consideration, on the features of the direct subject of criminal encroachment and opportunities to protect closed information resources by criminalistics methods, techniques and means.

When studying the process of cybercrimes investigation, Burbello (2013) notes that the primary task for an investigator at the initial stage of the investigation is to analyze the information environment of the crime:

- determining the type of the electronic computer (data storage device), where the illegally accessed computer information was stored or processed (Web-server, personal computer, mobile phone, electronic credit card), which will determine the direction of all further investigation;

- establishing the type of a computer operating system (server) that was illegally accessed (Unix, Linux, Netware, Windows), as well as the software used to commit the crime, which will greatly help narrow the circle of possible suspects;

- identification of hardware and software that has been affected during unauthorized access, as well as information about the means and tools of such access, which will provide a true picture of the traces of the crime.

When investigating cybercrime in the banking sector, it should be noted that it is committed by individuals with a high level of intellectual development and a high level of knowledge and skills in the field of software and computer technology. Therefore, as it was nicely noted by Muliar and Hovpun (2019), during the investigation of such crimes, it is advisable to involve experts and specialists in this field, who will be able to conduct an appropriate examination. A detailed description of the research conducted and the conclusion made by the authorized entity can be considered to be the expert's opinion. Such a person is an expert who has special knowledge in the relevant field according to which an expert investigation is commissioned. Examination is a kind of evidence, and therefore occupies a special place in the process of cybercrime proving.

It is advisable to use the experience of other countries concerning prevention, detection, cessation and investigation of cybercrime in the banking sector. Markov (2015) notes that creation of special anti-cybercrime units is common in many countries, including Australia, Belgium, Belarus, Britain, Denmark, Estonia, India, Canada, Malaysia, the Netherlands, Germany, Norway, Poland, USA, Switzerland, Sweden and others (p. 109).

The main functions of such units are: monitoring of cyberspace to detect cybercrimes, viruses or malware; taking of operation and investigation measures to record the illegal activities of cybercriminals; providing methodological and practical assistance to other sectoral services and law enforcement agencies within their competence; the accumulation, synthesis and analysis of cybercrime information; preventing cybercrime with the help of the public and mass communication (Markov, 2015).

It should also be noted that it is necessary to conduct temporary access to the stuff and documents as a measure to ensure criminal proceedings during the investigation of cybercrime in the banking sector (if necessary, the seizure of documents). Temporary access to stuff and documents means providing by the person possessing such things and documents the opportunity for the party to the criminal proceedings to get acquainted with them, make copies and,

in case of a decision by the investigating judge, court, to seize them (to make a seizure). Taking the specified action provides reception of stuff or documents, which can be used as evidence, having established their involvement in a cybercrime (Muliar & Hovpun, 2019).

It should be also mentioned that the UN has the International Telecommunication Union, functioning as a specialized agency, which was founded in 1865 as the International Telegraph Union, but it became a specialized UN agency in 1947. Its main areas include issues concerning information environment violations research. In this regard, the International Telecommunication Union implemented the program "Global Cybersecurity Agenda" in 2007 (ITU Global Cybersecurity Agenda), aimed at maintaining security and openness in the information society of the 21st century. This program operates on the basis of five basic principles:

- legislative measures;

- technical and applied initiatives;

- organizational structuring;

- capacity development in the information environment;

- international cooperation in this area (Schjølberg, 2008).

The analysis of the cybercrime investigation practice in the banking sector shows that it is necessary to introduce a new approach to detecting and investigating cybercrime as the measures and methods applied to document traditional crimes are not effective in this area. Thus, the field of high technology requires scientific, technical and other special knowledge not only of specialists, but also of operatives, investigators, prosecutors, investigating judges and judges. In this regard, special attention should be paid to increasing the level of professional training of the relevant operational units, pre-trial investigation bodies and a prosecutor. This is due to the fact that the insufficient level of this training can and does lead to errors in the application of criminal procedure and criminal law (Borysov & Zelenetskyi, 2010).

International cooperation should be carried out in several areas and include, first of all, the creation of regulations and standards and the development of general recommendations, as well as the introduction of effective models of organizational interaction between the states. In this respect, consideration must be given to the fact that traditional mechanisms of international cooperation, including inquiries, mutual assistance and other similar tools, which were used in the past, are not effective today, when crimes can occur from anywhere in the world at the speed of light (Smith, 2004).

Rohatiuk (2015) notes that the lack of a sufficient number of qualified personnel in law enforcement agencies makes it difficult to take quick and prompt decisions in criminal proceedings related to cybercrime. In addition to the above, investigators and prosecutors have problematic issues during the investigation of these crimes due to:

- the transition of most users from fixed access to the World Wide Web to mobile devices (gadgets);

- the use of closed TOR networks by the members of international criminal organizations, which makes it impossible to obtain relevant results by conducting covert investigative (search) activities;

- unavailability of an international cybercrime database;

- high latency of these types of crimes, as financial institutions (banks) do not want to advertise the facts of illegal interference with the work of their institution in order to preserve their own image;

- insufficient number of state experts in the field of computer analysis.

This situation needs to be constantly updated, the existing methods of cybercrime investigation should be updated, and new methods of cybercrime investigation in the banking sector should be developed.

2. GENERALIZATION OF THE MAIN STATEMENTS

In Ukrainian legislation, prior to the adoption of the Law of Ukraine On the Basic Principles of Cyber Security in 2017, there was no definition of cybercrime. According to the provisions of this Law, cybercrime (computer crime) is a socially dangerous criminal act in cyberspace and/or with its 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.

Today, an important aspect in the investigation of cybercrime in the banking sector is rapid and timely exchange of information, which will help increase the efficiency of the investigation process. To do this, it is necessary to establish communication between operatives, investigators, prosecutors and the court in order to quickly identify a criminal, collect information on the movement of information, use of software on applications and reports entered into the Unified Register of Pre-trial Investigations. It is also important to create a special database that will contain electronic evidence due to which the cybercrime investigation will be conducted properly.

The investigation of crimes committed in the cyberspace begins from the moment when the information was entered into the Unified Register of Pre-trial Investigations on the fact of detection of such a crime, and ends with drawing up an indictment against the person guilty of the crime and taking this person to court, or accordingly, the closure of criminal proceedings. At the pre-trial investigation stage, an investigator and a prosecutor apply various measures to take the perpetrators to court for crimes committed in cyberspace by conducting public and covert investigative (search) actions, appointing an expert investigation, and within the framework of international cooperation.

Cybercrime is increasingly encroaching on the bank accounts not only of companies or organizations, but also of ordinary citizens. With the increased number of non-cash payments, the number of victims of cyber fraud is growing. Factors contributing to the growth of cybercrime are the development and improvement of IT technologies, significant geography for committing crimes, insufficient theoretical and practical training of law enforcement officers and imperfection of domestic legislation.

In this respect, it should be noted that it is important for Ukraine not just to improve the legislation in the field of combating cybercrime, but also to take into account the human factor. The country's cybersecurity depends on the activities of the state to a greater extent, but specialists working in the field of prevention, counteraction and investigation of cybercrime play a significant part in creating an effective cybersecurity system. It takes time to settle the issue concerning improving the skills of law enforcement officers in the field of IT technologies. One of the variants to solve this issue may be involvement of specialists – programmers, developers of applications for payment for goods and services, software testers, system analysts, cybersecurity specialists. The leading activity of these specialists contributes to constant professional growth and updating of skills in line with technology changes. Interaction of law en-

Data in % according to the results of polling
of more than 5,000 respondents in 99 countries

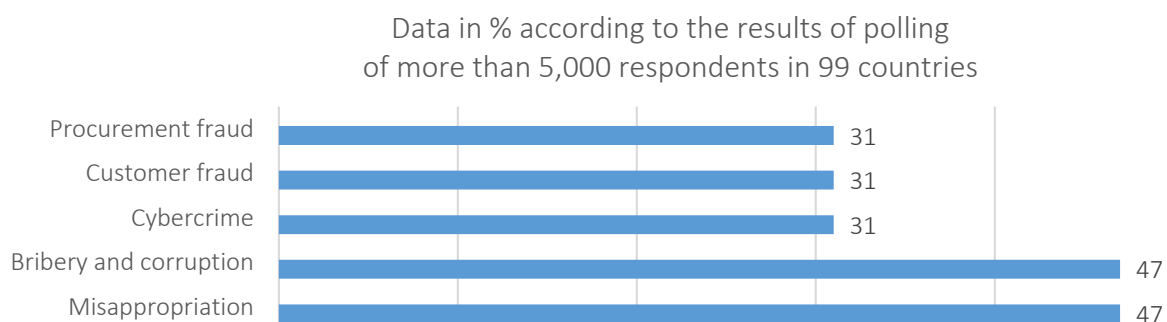| Type	Value
Procurement fraud	31
Customer fraud	31
Cybercrime	31
Bribery and corruption	47
Misappropriation	47

Figure 1. Top 5 types of fraud in the world according to the results of the PwC survey in 2020

forcement officers with IT specialists will partially solve the issue of investigating crimes in the banking sector in cyberspace.

In the context of improving the legal regulation of cybercrime investigation in the banking sector, it is currently important for Ukraine to adopt the experience of countries with effective cybersecurity systems. One of such measures is the introduction of the concept of "banking criminal law", aimed at regulating relations in the field of prevention, combating and investigation of cybercrime.

A significant number of banking institutions in Ukraine prefer overcoming the cybercrime consequences, rather than investing in the search for protection of data and accounts of their customers. The most common crimes in the banking sector is fraud using payment cards and their details, unauthorized debiting of bank accounts, interference with Internet banking, the spread of computer viruses, DDoS-attacks on Internet resources, fraud in information networks.

The practice of investigating cybercrimes in India, where professional hackers may be involved in the process, is interesting in the context of research. In many countries now there are so-called Cyber Corps, whose activities are aimed at protecting the country's cyberspace. Such corps operate in Germany, Russia, Britain, Estonia, the United States, and China. For example, in Germany, the Cyber Corps currently consist of 260 IT specialists; the smallest unit in this army is a unit whose activities are aimed at attack. The Estonian Cyber Corps consists of 300 people. There is a tendency to increase the number of cyber corps to increase the level of cybersecurity.

Foreign countries are actively using technological solutions to combat transnational cybercrime. Thus, back in 2011, Europol introduced to the EU members the IOCTA system (Internet Facilitated Organized Crime Tread Assessment), which facilitates the cybercrime detection. Now Europol provides investigative and analytical support to EU members through its online investigation system and crime database. The following example of transatlantic cooperation is illustrative. For example, two leading online anonymous markets, Alpha Bay and Hansa Market, were blocked by the Federal Bureau of Investigation (FBI) and the Dutch National High-Tech Crime Unit (NHTCU) during "Bayonet" Operation (according to Europol). The FBI managed to disrupt AlphaBay operation, a well-known darknet, and the NHTCU intervened in Hansa's darknet market for almost a month as an administrator and then shut down Hansa Market forever. Many AlphaBay users sought refuge at the Hansa market, where the NHTCU was operating at that time. Thus, police agencies were in an ideal position not only to disrupt the ecosystem by creating mistrust among users of these anonymous markets, but also to collect valuable data from thousands of them (Wegberg & Verburgh, 2018).

International cooperation in regards to cybercrime combating must be carried out based on the participation of all countries, which is determined by the nature of the information itself as an object of encroachment, and the nature of the crimes committed. According to Stein Schjolberg, an international expert in the field of the cybercrime legislation harmonization, "cyberspace, as the fifth common space, after land, sea, air and outer space, requires coordination, cooperation and special legal measures at the international level" (Schjolberg, 2010). Indeed, in today's world, all spheres of life are directly dependent on the operation of computer and information networks.

There is a Cybersecurity Strategy in Ukraine, approved by the President of Ukraine in 2016, according to which anti-cybercrime activities should include, in particular, the implementation of measures to improve procedural mechanisms for collecting evidence relating to crime, in electronic form, improving classification, methods, tools and technologies of cybercrime identification and recording, conducting expert research.

Cybercrime can violate the interests of both the state and the individuals. Undoubtedly, the peculiarities of information systems functioning, especially the Internet, "require the cybersecurity issues to be solved by the joint efforts of various entities, both public and private" (Huey et al., 2013), but it is the state that can and should, and most importantly, only the state can effectively carry out full-scale counteraction to the cybercrime commission, create conditions for those who are
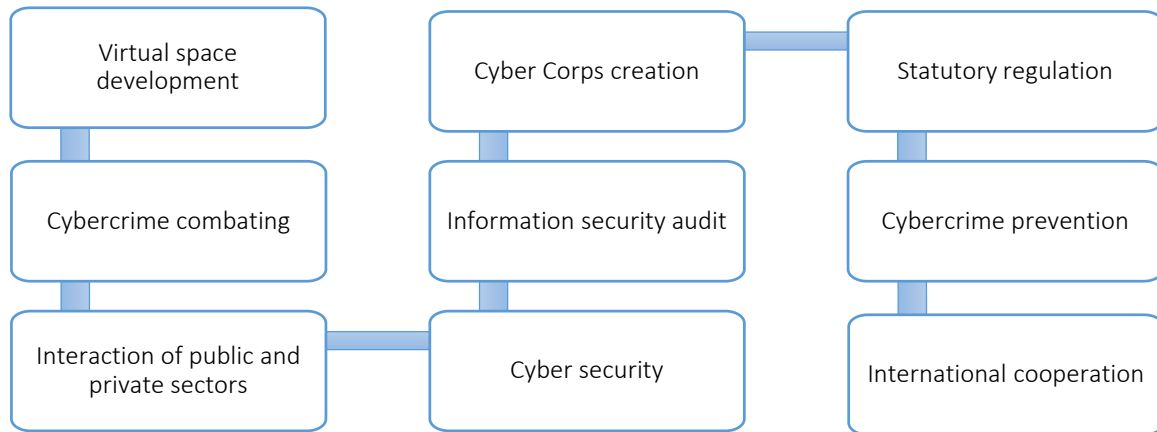
Figure 2. Approaches to increasing the level of cybersecurity in Ukraine

the most vulnerable to cybercrime attacks (for example, banks, individuals), so that they can build a more reliable system of information protection.

One of the topical issues of modern Ukrainian society is the bureaucratization of law enforcement bodies. The investigation of cybercrime is delayed because of the need to coordinate the activities of different departments, operational groups, an investigator and a prosecutor. The large number of documents required for operational and investigative actions delays the process, and consequently evidence and traces of the crime may be lost. Improving the process of cybercrime investigation in the banking sector and improving cybersecurity in Ukraine can be achieved through the creation of a special unit – cyber forces, whose activities will be aimed at preventing the commission of crimes in cyberspace. This will significantly reduce the number of fraudulent acts and crimes in the field of banking operations.

CONCLUSION

In modern Ukraine, there is no effective system for combating cybercrime in the banking sector; The solution to this issue is possible through the development of measures aimed at preventing and effectively investigating crimes committed in cyberspace. The analysis of the experience of the world's leading countries shows that the basis of an effective system for combating cybercrime in the banking sector is the coordinated activity of public and private sectors on the following vectors:

1) enshrining the classification of cybercrimes in Ukrainian regulatory legal acts and establishing clear responsibility for each type of crimes committed in cyberspace;

2) introducing the concept of "banking criminal law" in the scientific and legal spheres, which is due to the rapidly growing high level of cybercrime in the banking sector;

3) establishing cooperation between banking institutions, government and law enforcement agencies both in terms of interaction models and increasing the level of trust of the private sector to government officials and law enforcement officers, which will help reflect real statistics of cybercrime committed in the banking sector and increase the effectiveness of its investigation;

4) creation of Ukrainian cyber forces, whose activities will be aimed at preventing and combating crimes committed in cyberspace.

Thus, the analysis of the practice of creating an effective cybersecurity system allows us to assert that properly coordinated activities of the public and private sectors will contribute to minimization of cybercrimes committed in the banking sector and increase the level of the virtual space security in Ukraine.

AUTHOR CONTRIBUTIONS

Conceptualization: Oleksii M. Skriabin, Oleksandr N. Kurakin.
Data curation: Pavlo S. Pokataev, Oleksandr N. Kurakin.
Formal analysis: Pavlo S. Pokataev, Oleksii M. Skriabin.
Investigation: Oleksandr N. Kurakin, Dmytro B. Sanakoiev.
Project administration: Sergey S. Vitvitskiy.
Resources: Pavlo S. Pokataev, Dmytro B. Sanakoiev.
Supervision: Sergey S. Vitvitskiy.
Writing – original draft: Oleksii M. Skriabin, Sergey S. Vitvitskiy.
Writing – review & editing: Oleksii M. Skriabin, Dmytro B. Sanakoiev.

REFERENCES

1. Ajkov, D., Sejger, K., & Fonstorh, U. (1999). *Kompyedternyye prestupleniya. Rukovodstvo po borbe s kompyuternymi prestupleniyami [Computer crimes. A Guide to Combating Computer Crime]* (351 p.). Moscow: Mir. (In Russian). Retrieved from http://bek.sibadi.org/fulltext/ed1014.pdf

2. Ben-Itzhak, Y. (2008). Organized Cybercrime. *ISSA Journal, 6*(10), 37-48. Retrieved from https://mydigitalpublication.com/publication/?m=1336&i=6393&p=37&ver=html5

3. Bissel K., LaSalle, R. M., & Richards, K. (2017). *The Assenture Security Index. Redefining Security Performance and How to Achieve it.* Retrieved from https://www.accenture.com/t20170213T002042__w__/us-en/_acnmedia/PDF-43/Accenture-The-Acn-Security-Index.pdf

4. Borisov, V. I., & Zelenec'kij, V. S. (2010). *Problemy zabezpechennia efektyvnosti diialnosti orhaniv kryminalnoho peresliduvannia v Ukraini [Problems of ensuring the effectiveness of criminal prosecution in Ukraine]* (400 p.). Kharkiv: Pravo. (In Ukrainian). Retrieved from http://library.nlu.edu.ua/POLN_TEXT/MONOGRAFII_2011/PERESLIDUVAN-NY_2010.pdf

5. Brenner, S. (2006). *Cybercrime: criminal threats from cyberspace* (281 p.). Praeger. Retrieved from https://www.researchgate.net/publication/266090469_Cybercrime_Criminal_Threats_from_Cyberspace

6. Buhtiarova, A. G., & Huscha, A. V. (2019). Combating Cybercrime in the Banking Sector. *Pryazovskyi ekonomichnyi visnyk – Priazovsky Economic Bulletin, 3*(14), 355-361. (In Ukrainian). Retrieved from http://pev.kpu.zp.ua/journals/2019/3_14_uk/60.pdf

7. Burbelo, B. A. (2013). Kryminalistychni osnovy protydii kiberzlochynnosti [Forensic foundations of combating cybercrime]. *Aktualni pytannia rozsliduvannia kiberzlochyniv: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii [Current issues cybercrime investigation: materials of the International scientific and practical conference]* (pp. 179-182). Kharkiv: Kharkivskyi natsionalnyi universitet vnutrishnikh sprav. (In Ukrainian). Retrieved from http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/553/Aktualni%20pytannia%20rozsliduvannia%20kiberzlochyniv_Materialy%20konferentsii_2013.pdf?sequence=1&isAllowed=y

8. Decree of the President of Ukraine. (2016). *Stratehiia kiberbezpeky Ukrainy [Cybersecurity strategy of Ukraine].* Retrieved from https://www.president.gov.ua/documents/962016-19836

9. Douschi, M. I. (2018). Pravove rehuliuvannia zabezpechennia kiberbezpeky v Ukraini [Legal regulation of cyber security in Ukraine]. Proceedings of the *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia [Cybersecurity in Ukraine: legal and organizational issues: materials of the All-Ukrainian scientific-practical conference]* (pp. 21-23). Odesa: ODUVS. (In Ukrainian). Retrieved from http://oduvs.edu.ua/wp-content/uploads/2017/01/Kiberbezpeka-v-Ukrayini-final.pdf

10. Europol. (2011). *Threat Assessment on Internet Facilitated Organized Crime (IOCTA).* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/threat-assessment-internet-facilitated-organised-crime-iocta-2011

11. Europol. (2017). *Massive blow to criminal Dark Web activities after globally coordinated operation.* Retrieved from https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

12. Giovanni Paolo Accinni e As-

sociati. *Banking Criminal Law.* Retrieved from http://www.studio-accinni.com/banking-criminal-law-en.htm

13. Hilgendorf, E., & Valerius, B. (2012). *Computer- und Internetstrafrecht.* Springer: Verlag Berlin Heidelberg. https://doi.org/10.1007/978-3-642-16885-7

14. Huey, L., Nhan, J., & Broll, R. (2013). Uppity civilians and cyber-vigilantes: The role of the general public in policing cybercrime. *Criminology and Criminal Justice, 13*(1), 81-97. https://doi.org/10.1177/1748895812448086

15. Ismailov, K., & Shaevskaya, Ju. V. (2016). Kiberzlochynnist finansovoi sfery Ukrainy [Cybercrime in the financial sphere of Ukraine]. Collection of scientific articles based on the reports of the participants of the *All-Ukrainian scientific-practical conference* (pp. 134-139). Odesa: ODUVS. (In Ukrainian).

16. Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2015). Cybercrime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149-164). Waltham. Retrieved from https://cdn.ttgtmedia.com/rms/security/Cyber-Crime-and-Cyber-Terrorism-Ch12.pdf

17. Janke, G. (2008). *Kompendium Wirtschaftskriminalitat.* Peter Lang GmbH International Verlag der Wissenschaften. Frankfurt am Main.

18. Kroes, N. (2013). *Speech: EU Cybersecurity Strategy.* Retrieved from http://europa.eu/rapid/press-release_SPEECH-13-51_en.htm

19. Leonov, B. D., & Serʼogin, V.S. (2019). Udoskonalennia metodychnoho zabezpechennia ekspertnykh doslidzhen spetsialnykh prohramnykh zasobiv u sferi protydii kiberzlochinnosti [Improving the methodological support of expert research of special software in the field of combating cybercrime]. *Informatsiia i pravo – Information and Law, 4*(31), 98-106. (In Ukrainian). https://doi.org/10.37750/2616-6798.2019.4(31).194758

20. Marbeth-Kubicki, A. (2010). *Computer- und Internetstrafrecht.* München: Verlag C. H. Beck.

21. Markov V. V. (2015). Do pytannia shchodo zarubizhnoho dosvidu protydii kiberzlochynnosti [On the issue of foreign experience in combating cybercrime]. *Pravo i bezpeka – Law and security, 2*(57), 107-113. (In Ukrainian). Retrieved from http://nbuv.gov.ua/UJRN/Pib_2015_2_23

22. Mazzone, A. (2006). *Identity Fraud – Government Legislative Responses.* Victorian Government Solicitor's Office. Retrieved from http://vgso.vic.gov.au/sites/default/files/publications/Identity%20Fraud%20-%20Government%20Legislative%20Responses.pdf

23. Miles, T. (2017). *U.N. survey finds cybersecurity gaps everywhere except Singapore.* Reuters. Retrieved from https://www.reuters.com/article/us-cyber-un/u-n-survey-finds-cybersecurity-gaps-everywhere-except-singapore-idUSKBN19Q19L

24. Muhin, G. N., & Isjutin-Fedotkov, D. V. (2013). Osobennosti struktury i soderzhaniya metodiki rassledovaniya prestupleniy, svyazannykh s posiagatelstvom na informatsionnyye resursy [Features of the structure and content of the methodology for investigating crimes related to infringement of information resources]. *Biblioteka kriminalista – Forensic Library, 5,* 280-286. (In Russian). Retrieved from https://scholar.google.ru/citations?user=rb2kJrwAAAAJ&hl=ru

25. Muliar, G. V., & Khovpun, O. S. (2019). Features of evidence of cybercrime. *Law. Human. Environment, 10*(3), 132-138. (In Ukrainian). http://dx.doi.org/10.31548/law2019.03.017

26. Nekrasov, V. (2016). *Lehki hroshi: Ukraina peretvoriuietsia na Mekku dlia kiberzlochyntsiv [Economic truth. Easy money: Ukraine is becoming a Mecca for cybercriminals].* (In Ukrainian). Retrieved from https://www.epravda.com.ua/publications/2016/03/28/587004/

27. Odenthal, R. (2009). *Korruption und Mitarbeiterkriminalitat: Wirtschaftskriminalitat vorbeugen, erkennen und aufdecken.* Springer Gabler, Wiesbaden. http://dx.doi.org/10.1007/978-3-8349-8795-2

28. Pushkarenko, P. I. (2006). Kiberzlochynnist yak novitnii fenomen tiniovoi ekonomiky [Cybercrime as a new phenomenon of the shadow economy]. *Problemy i perspektyvy rozvytku bankivskoi systemy Ukrainy – Problems and prospects of development of the banking system of Ukraine, 17,* 75-82. (In Ukrainian). Retrieved from https://essuir.sumdu.edu.ua/handle/123456789/55998

29. Rogatjuk, I. V. (2015). Rozsliduvannia kiberzlochiniv: okremi aspekty diialnosti prokurora i slidchykh orhaniv vnutrishnikh sprav [Investigation of cybercrime: some aspects of the activities of the prosecutor and investigative law enforcement agencies]. *Aktualni pravovi pytannia siohodennia v umovakh yevrointehratsii Ukrainy [Current legal issues in the context of Ukraine's European integration]* (pp. 18-21). (In Ukrainian). Retrieved from http://elar.naiau.kiev.ua/jspui/handle/123456789/6798

30. Schjølberg, S. (2008). *Report of the Chairman of HLEG.* ITU Global Cybersecurity Agenda (GCA). Retrieved from https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

31. Schjolberg, S. (2010). A cyberspace treaty – A United Nations convention or protocol on cybersecurity and cybercrime. *Twelfth United Nations Congress on Crime Prevention and Criminal Justice.* Salvador, Brazil. Retrieved from http://cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf

32. Sen, R. Ju. (2014). Dosvid inozemnykh krain u sferi rozsliduvannia kiberzlochyniv [Experience of foreign countries in the field of cybercrime investigation]. *Aktualni pytannia diialnosti pravookhoronnykh orhaniv u sferi protydii kiberzlochynnosti. Materialy Mizhnarodnoi naukovo-praktychnoi konferentsii [Current issues of law enforcement in the field of combating cybercrime:*

materials of the international scientific-practical conference] (pp. 192-194). Kharkiv: Prava liudyny. (In Ukrainian). Retrieved from http://dspace.univd.edu.ua/xmlui/handle/123456789/408

33. Sindhu, K. K., Kombade, R., Gadge, R., & Meshram B. B. (2012). Forensic Investigation Processes for Cyber Crime and Cyber Space. *Proceedings of International Conference on Internet Computing and Information Communications* (pp. 193-206). https://doi.org/10.1007/978-81-322-1299-7_19

34. Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Criminals on Trial* (263 p.). Cambridge University Press.

35. Steele, J. (2020). *Credit card fraud and id theft statistics*. Retrieved from https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/

36. Stein, A. R. (2004). Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulator Precision. *Northwestern University Law Review, 98*(2), 411-454. Retrieved from https://search.proquest.com/docview/233345729

37. The Verkhovna Rada of Ukraine. (2017). *Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbez-peky Ukrainy [Law of Ukraine On the Basic Principles of Cyber Security in Ukraine].* Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text

38. Wegberg, R., & Verburgh, T. (2018). Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. In *Evolution of the Darknet Workshop at the Web Science Conference (WebSci 18)* (pp. 1-5). Association for Computing Machinery (ACM). Retrieved from http://pure.tudelft.nl/ws/portalfiles/portal/46185682/Wegberg_Verburgh_Lost_in_the_Dream.pdf