DOI: https://doi.org/10.34069/AI/2022.53.05.26

How to Cite:
Pohoretskyi, M., Cherniak, A., Serhieieva, D., Chernysh, R., & Toporetska, Z. (2022). Detection and proof of cybercrime. *Amazonia Investiga*, *11*(53), 259-269. https://doi.org/10.34069/AI/2022.53.05.26

# Detection and proof of cybercrime

## Виявлення та доказування кіберзлочинів

Received: April 3, 2022 Accepted: May 5, 2022

Written by:
**Mykola Pohoretskyi**[111]
https://orcid.org/0000-0003-0936-0929
**Andrii Cherniak**[112]
https://orcid.org/0000-0003-1803-0673
**Diana Serhieieva**[113]
https://orcid.org/0000-0003-1005-7046
**Roman Chernysh**[114]
https://orcid.org/0000-0003-4176-7569
Web of Science researcher code: AAV-4639-2020
**Zoriana Toporetska**[115]
https://orcid.org/0000-0002-2441-4852

**Abstract**

Analysis findings in the field of cybercrime in the world and Ukraine as well prove a steady trend towards its growth, which causes a systematic increase in the number of victims affected by illegal malpractice of cyber criminals. This negative phenomenon violates not only citizens' interests guaranteed by law, but also poses a threat to the national security in many countries. At the same time, international order is undermined and sustainable interstate relations are violated.

Rapid information system development, speedy progress of computer software and hardware prompt numerous crimes in this field. Cybercrimes are committed by trained persons with a high intelligence level and professional knowledge in the computer technology sphere. In accordance with foregoing the issue of law approximation and the procedure of identification and recording of the mentioned illegal activity is essential to eradicate cybercrime.

Considering the fact that the category of "proof" is fundamental in the theory of criminal procedure, we build in general-theoretical approaches in the basics of the analysis of the

**Анотація**

Результати аналізу ситуації у сфері кіберзлочинності у світі та Україні, свідчать про сталу тенденцію до її зростання, що зумовлює системне збільшення кількості потерпілих від протиправних дій кіберзлочинців. Вказане негативне явище порушує не лише охоронювані інтереси громадян, а й становить загрозу національній безпеці багатьох країн. При цьому дестабілізується міжнародний порядок і порушується стале функціонування міждержавних відносин.

У зв'язку із стрімкою інформатизацією людства, надшвидким розвитком комп'ютерних систем і технологій, злочини у вказаній сфері прогресують. Кіберзлочини вчиняються підготовленими особами, які мають високий інтелектуальний рівень та фахові знання з використання комп'ютерних технологій. З огляду на викладене, актуальним є питання оптимізації положень законодавства та вдосконалення механізму виявлення і документування зазначеного виду протиправної діяльності для її припинення.

[111] Doctor of Science in Law, Professor, Vice-rector for scientific and pedagogical work, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
[112] Doctor of Science in Law, Professor, Rector of the National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[113] Doctor of Science in Law, Senior Research Fellow, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
[114] Ph.D (Law), Associate Professor of the Department of Science of Law, National Academy of the Security Service of Ukraine, Kyiv, Ukraine.
[115] Ph.D (Law), Associate Professor, Associate Professor of the Department Criminal Procedure and Criminalistics Department, Educational and Scientific Law Institute, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.



Creative Commons Attribution 4.0 International (CC BY 4.0)

procedure of cybercrimes identification and recording to the mentioned activity in general.

**Key words:** proof, the process of proof, pretrial investigation, cyberspace, Internet network, cybercrime.

Зважаючи на те, що категорія «доказування» є фундаментальною в теорії кримінального процесу, в основу аналізу процедури виявлення та формування доказової бази в ході документування кіберзлочинів нами закладено саме загальнотеоретичні підходи до вказаної діяльності у цілому.

**Ключові слова:** доказування, досудове розслідування, кіберпростір, мережа Інтернет, кіберзлочин.

## Introduction

It is impossible to imagine our modern world without digital gadgets, messengers, Internet banking, the Internet, databases, etc., which are used in everyday life and professional activities on a daily basis (Chernysh, Pogrebnaya, Montrin, Koval and Paramonova, 2020). The processes of informatization and digitalization have led to the formation of a global information space.

Criminal procedure has also fallen under the influence of digital progress – criminal offences are committed in cyberspace with ever increasing frequency (Komarova, Kaluhina, Pohoretskyi, Hribov & Cherniak, 2020).

The daily operation of banking and energy systems, air traffic control, transport network, ambulance, etc. are entirely dependent on the reliable and secure operation of automated electronic computer systems. Today it is possible to predict a further increase in the dependence of national infrastructure on the informatization processes and Ukraine's entry into a single information space, the spread of criminogenic processes related to the illegal use of computer technology (Kirbyatyev, 2010).

Cybercrime is an international phenomenon. The analysis of the spread of cybercrime in the world and in Ukraine attests to a consistent trend towards its growth, which leads to a systematic increase in the number of victims of illegal actions of cybercriminals (Kostenko, Strilchuk, Chernysh, Buchynska, & Fedoronchuk, 2021). In particular, according to official Interpol statistics, cybercrime is one of the fastest growing crime areas (ICED, 2018). The report of the European Police Office (Europol) "The Internet Organized Crime Assessment (IOCTA)" states that according to the European Union member states' statistics, the number of registered cybercrimes reaches or even exceeds the number of traditional crimes (IOCA, 2018).

We state that the statistics indicating the cybercrime growth are directly proportional to the level of development and implementation of modern computer technology, public networks and their availability.

This negative phenomenon not only violates the citizens' protected interests, but also poses a threat to the national security of many countries. Concurrently, the international order is destabilized and the sustainable functioning of interstate relations is disrupted (Svitlana, Onyshchuk, Petroye and Chernysh, 2020).

Cybercrime causes significant economic damage. In particular, according to experts, in 2020 the total amount of financial damage caused by the mentioned above illegal acts exceeded one trillion US dollars, which is more than 1% of world gross domestic product (Sviatun, Goncharuk, Chernysh, Kuzmenko and Kozych, 2021). As it has been noted by Wicki-Birchler, if cybercrime were compared to a country, it would be the 13th largest economy in the world in terms of gross domestic product, just ahead of Australia and Spain (Wicki-Birchler, 2020).

Due to the rapid informatization of mankind, extremely rapid development of computer systems and technology (Figure 1) crimes in this field are progressing.

In view of the above, the issue of optimizing the legislation provisions and improving the mechanism for detecting and documenting this type of illegal activity in order to stop it is highly relevant.



Creative Commons Attribution 4.0 International (CC BY 4.0)

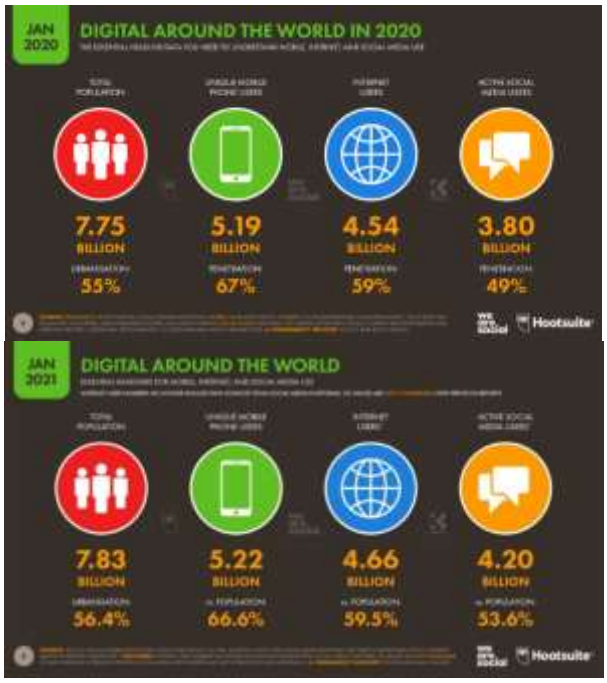


***Fig. 1.*** Digital 2020/2021: global overview report (Datareportal, 2021)

One of the stages of domestic legislation adoption to international and European standards was the updating of criminal procedure legislation of Ukraine in 2012: the procedural form of prejudicial inquiry was changed, court functions were expanded to control human rights and freedoms. Besides, approaches to the evidentiary process in criminal proceedings have changed significantly (Ponomarenko, Havryliuk, Anheleniuk & Drozd, 2020).

The scientific category of "proof" is one of the most studied. Most scholars recognize it as an independent scientific category of the criminal procedure.

It is believed that the proof in criminal procedure is a complex objective-subjective activity consisting of a number of interdependent and interrelated elements based on the formation of the proof base (Pohoretskyi, 2007).

However, there is a lack of consensus among lawyers on certain elements of this theory. In particular, the following issues remain controversial: the methodological bases of proof, the correlation between proof and cognition, expediency of using the theory of reflection in the theory of proof, the purpose and the results of proof, the means and the subjects of proof, etc. The ambiguity of scientific approaches to most fundamental categories in the theory of proof leads to the fact that lawmakers and law enforcers face certain problematic issues in the process of their application. This, in general, has a negative impact on the effectiveness of legal provisions implementation.

The process of proof is a separate procedural mechanism that requires systematic improvement taking place in accordance with social relations development. Taking into account all the above, one of the main priorities for Ukraine is to develop effective national legislation that will ensure the implementation of citizens' constitutional rights and freedoms and will be aimed at preserving statehood by combating external and internal threats in the information space. Thus, the issue of cybercrime detection and investigation (including the formation of evidence base) requires further thorough theoretical development.

**Theoretical framework**

Bearing in mind that the category of evidence is fundamental in the theory of criminal procedure; we build in general theoretical approaches to this activity by and large as the basis of the analysis of this procedure for detecting and forming the evidence base for documenting cybercrime.

Problematic issues of "proof" as a theoretical category have been studied in scientific works by leading domestic and foreign experts in the field of criminal procedure, in particular: Gmirko, V., Loboyko, L., Pohoretskyi, M., Sibilova, N., Stakhivsky, S., Cherniak, A, Shumylo, M., etc.


Creative Commons Attribution 4.0 International (CC BY 4.0)

However, given the dynamic change in public relations, it is necessary to improve procedural skills for relevant documentation of illegal activities and, accordingly, to sue perpetrators.

We share the views of those scholars who recognize the existence of the theory of criminal procedural proof as an independent theory of criminal procedure and, at the same time, they claim that the theory of proof is a part of it.

The results of the analysis of modern scientific works by Ukrainian authors on the theory of proof, as well as foreign experts who influence the development of domestic theory of proof, give grounds to highlight three main scientific concepts, which present currently the theory of criminal procedural evidence in the post-Soviet space.
The most common of these is the concept of considering proof as a criminal procedure for collecting, verifying and evaluating evidence (Loboyko, 2005; Stakhivsky, 2005; Sibilova, 1990).

This concept, in our opinion, does not fully correspond to the essence of criminal procedural proof of adversarial or mixed criminal proceedings.

Another one is the theoretical concept of criminal procedural proof, which is based on system-thinking methodology (STM) (Gmirko, 2011; Shumylo, 2013).

The main reason for the inconsistency of the theoretical concept of proof using STM in the modern model of the criminal process in Ukraine is that its supporters could not interpret properly the philosophical system-thinking methodology. Some provisions of the methodology are controversial in philosophy and theory of activity, in criminal procedural theory. Its implementation in developing the author's concept of criminal procedural proof taking into account the modern model (type, form) of the criminal process of Ukraine, procedural functions of the parties to criminal proceedings and the court in this model, as well as the needs of the modern domestic law enforcement practice remains problematic.

The scientific concept of criminal procedural proof is also worth mentioning, since its followers argue that the contemporary mixed criminal process is of investigative essence and therefore suggest a "competitive paradigm of proving the truth and its inherent information-communicative model of interaction of participants in preliminary (pre-trial) and judicial investigation" instead (Aleksandrov, 2010).

In our opinion, the relevance of introducing the concept of adversarial system of criminal procedural evidence into the Ukrainian current legal system is a controversial issue. Moreover, in recent decades in the United States, Great Britain and other countries which have a common law system, the powers of pre-trial agencies are expanded and strengthened due to significant changes in criminal activity (organization, professionalism, transnationality, increased public vulnerability, etc.) and the emergence of new crimes (including cybercrime). Such legal policies of Western democracies are in line with the concept of "Crime control", which in recent decades has dominated the concept of "Protection of human rights" (Pohoretskyi, 2004).

At the same time, regardless of our critical remarks on the above mentioned concepts of criminal procedural proof, we state that each of them is of a remarkable scientific and practical value, influences the development of any other concepts or constitutes their basis, and therefore requires more in-depth research.

Introducing our own concept of criminal procedural proof in the scientific article (due to the limited volume of publication) we assume that criminal procedural proof is a cognitive-practical and mental (logical-psychological) activity.

We believe that the concept of criminal procedural proof is based on the form (type, model) of the domestic criminal process, which is implemented by the current Criminal Procedure Code of Ukraine (hereinafter CPC of Ukraine), as well as three classic criminal procedural functions – prosecution, defense, trial and resolution (administration of justice). This is the basis of the criminal process and, in particular, the criminal holistic inseparable process, which consists of obtaining and using evidence (Pohoretskyi, 2015).

**Methodology**

According to the purpose of the article, a number of scientific methods of modern epistemology were used in the scientific research. The methodological basis of the study was the theory of cognition of legal provisions, which were developed by prominent experts in the field of criminal procedural law. Over and above special research methods were used, in particular:


Creative Commons Attribution 4.0 International (CC BY 4.0)

comparative – to compare the rules of criminal substantive and procedural law; historical and legal – for retrospective analysis of the concept of the essence of criminal procedural proof and the process of establishing scientific views on the issue; special legal – for a thorough analysis of regulations governing the procedure of detection and proof; systematic approach, and logical-legal method – to analyze the impact of negative factors on the constituent elements of the formation of logical and specific theoretical and applied conclusions.

**Results and discussion**

Before proceeding to the consideration of problematic issues related to the detection and proof of cybercrime, it should be noted that the definition of the concept and the signs of cybercrime and cyber criminality in Ukrainian criminal law is still under discussion, because at the national level this concept has no legislative definition.

This is due to the fact that it is "relatively young" for the science of criminal law.

Among the first international regulations that enshrines the definition of "cybercrime" and forms the idea of crimes in cyberspace was The Convention on Cybercrime (adopted by the Council of Europe in 2001 and ratified by Ukraine in 2005; hereinafter referred to as the Budapest Convention). In this regulatory document, cybercrimes are divided into 5 groups: 1) crimes against the confidentiality, integrity and accessibility of computer data and systems (illegal access, illegal interception, data interference, interference with the system); 2) crimes related to the use of a computer as a means of committing crimes, namely, for the manipulation of information (computer fraud and computer forgery); 3) crimes related to the content (content of the data); 4) crimes related to the violation of copyright and related rights; 5) acts of racism and xenophobia committed via computer networks (CETS, 2005).

Today, the Budapest Convention is a fundamental document for the development of international and national legislation regulating issues related to the fight against cybercrime.

The provisions of the above-noted statutory regulation require from member states of the Council of Europe and other states that have ratified it to take measures to:

– criminalize attacks on computer data and systems (i.e. illegal access, illegal interception, data interference, system interference, device misuse), as well as offenses committed with the use of personal computers (forgery and fraud), offenses related to content (child pornography) and offenses in the field of copyright and related rights;
– enhance the competence of special entities in the field of cybercrime investigation;
– improve the procedure of storing electronic evidence (urgent storage of computer data; urgent storage and partial disclosure of data on the movement of information; search and arrest of computer data; collection of data on the movement of information in real time; interception of data on the content of information, etc.);
– develop international cooperation with other countries which are parties to the Convention through general (extradition, mutual assistance, sharing of information, etc.) and special measures (urgent saving and disclosure of stored data on the movement of information, mutual assistance in access to computer data, cross-border access to computer data, creation of round-the-clock networks, etc.) (Law No. 2824-IV, 2005).

Analyzing the concept of "cybercrime", we note that among scientists there are no unified concepts regarding its content.

In particular, according to V. Butuzov, computer crimes and cybercrimes are different types of crimes in the field of information technology, the classification of which takes place on the following grounds:

1. The criterion of attribution of certain crimes to computer crimes is the instrument of committing a crime - computer equipment.
2. The object of encroachment is public relations in the field of automated information processing.
3. The criterion of attribution of crimes to cybercrimes is the specific environment for committing crimes, namely, cyberspace (environment of computer systems and networks) (Butuzov, 2010). In our opinion, the object of encroachment proposed by the scientist should be supplemented with public relations in the field of accumulation of information, and not only its processing.


Creative Commons Attribution 4.0 International (CC BY 4.0)

The dictionary of cybersecurity terms contains the following definitions of the concept of "cybercrime":

1. Cybercrime is a crime related to the use of cybernetic computer systems, and a crime in cyberspace.
2. Cybercrime is the most dangerous cyber violation for which criminal liability is established by law (Glossary of cybersecurity terms, 2012).

According to V. Bolgov, cybercrime is a set of criminally punishable socially dangerous acts (actions or inactions) stipulated by the current legislation, which encroach on the right to protection against unauthorized dissemination and use of information, negative consequences of the influence of information, or the functioning of information technology, as well as other socially dangerous acts related to the violation of ownership of information and information technology, the rights of owners or users of information technology to receive or disseminate reliable and complete information in a timely manner (Bolgov, 2015).

A common feature of the unlawful acts stipulated in the Convention and its Additional Protocol is that their commission at different stages is directly related to the use of computer systems resources (commission using computer systems or through computer systems), which, in turn, are the environment for committing cybercrimes. Cybercrimes should be considered those which are committed with the use of or through computer systems, or connected with computer systems, that is, with a set of devices from which one or more, in accordance with a particular program, perform automatic data processing (Pohoretskyi, 2012).

Without going into a thorough analysis of the theory and views on the definition of "cybercrime" and taking into account that the term "cybercrime" is made up of the words "cyber" (implying "cyberspace", "virtual world", "information space") and "crime" (Vasylkovsky, 2018), "cybercrime" can be defined as a socially dangerous act provided by the law on criminal liability, which is committed in cyberspace using electronic computing machines (computers), telecommunications systems, computer and telecommunications networks. At the same time, it should be borne in mind that such an act is directed against the rights and legitimate interests of participants in cyberspace (individuals, legal entities, states), which are protected by criminal and international law.

The Budapest Convention, as a fundamental document in the field of combating cybercrime, provides a provisional classification of cybercrimes, which are divided into offenses:

– against the confidentiality, integrity and availability of computer data and systems;
– related to computers, including computer forgery and fraud;
– related to the content of information. In particular, child pornography, racism and xenophobia; infringements related to copyright and related rights, such as illegal reproduction and use of computer programs, audio / video and other digital products, as well as databases and books (Order № 157, 2013).

The results of empirical data analysis show that today the main types of cybercrime committed in Ukraine are:

– theft of information and personal data;
– fraud with plastic payment cards or bank accounts;
– fictitious Internet auctions, as well as scams that occur in the field of purchase and sale of goods and services through free bulletin boards in cyberspace (sale of non-existent goods);
– fraud by creating fictitious sites of lottery operators, online casinos and sending advertising letters, informational messages with winning the lottery or offering free participation in the game in order to obtain personal data (phishing);
– redemption and registration of domain names (cybersquatting);
– theft of services (phone-cracking);
– the spread of viruses and malware.

One of the ways of committing illegal acts in the field under study is the global Internet, which is used to commit a significant part of illegal acts. The responsibility for these acts is provided by the Criminal Code of Ukraine.

As pointed out above, there is no comprehensive definition of "cybercrime" in the national law, there is only a generalized concept of crimes and offenses committed with the use of computers, computer systems and telecommunications networks.

In particular, the Criminal Code of Ukraine contains Chapter XVI "Crimes in the field of using electronic computing machines (computers), systems and computer networks." It


Creative Commons Attribution 4.0 International (CC BY 4.0)

enshrines the so-called "classic cybercrimes" (Law № 2341-III, 2001).

At the same time, a distinction which helps us attribute certain types of crime in the field of high technology to computer ones in general is the instrument of crime – computer technology and a sign of cybercrime is a specific environment for committing crimes – cyberspace (computer systems and networks). Of course, if we consider the group of crimes united in a separate section of the Criminal Code of Ukraine – "crimes in the field of using electronic computing machines (computers), systems, computer and telecommunications networks" separate from other forms of criminal behavior using computer technology and high technology, while assuming that they are not (not included) in a single network, such a classification makes sense (Kravtsova, 2015).

At the same time, according to N. Akhtyrska, this list includes some articles of the Criminal Code of Ukraine, which point out the methods used for committing a crime using a computer or information (automated) systems. In particular, the corpus delicti provided for by: Part 3 of Art. 190 of the Criminal Code of Ukraine, – "Fraud committed on a large scale or through illegal transactions using electronic computer"; Part 4 of Art. 301 of the Criminal Code of Ukraine – "Forcing minors to participate in the creation of works, images or film and video products, computer programs of pornographic nature"; Art. 200 "Illegal actions with documents for transfer, payment cards and other means of access to bank accounts, electronic money, equipment for their production", Art. 376-1 "Illegal interference in the work of the automated court document management system" (Akhtyrska, 2018). However, this list of illegal acts that contain signs of a crime is not comprehensive, as computer technology can be used while committing other crimes.

In the process of investigating "cybercrimes" the issue of conducting a comprehensive and expeditious pre-trial investigation of these criminal proceedings, collecting and consolidating the entire bulk of evidence, preserving the legal properties of evidence and further determining the person's guilt or innocence remain actual.

Evidence in criminal proceedings is actual data obtained in the CPC of Ukraine, on the basis of which the investigator, prosecutor, investigating judge and court establish the presence or absence of facts and circumstances relevant to criminal proceedings and subject to proof (Article 84 Part 1). Proving involves collecting, verifying and evaluating evidence in order to establish the circumstances relevant to criminal proceedings (Article 91 Part 2). The purpose of proving in criminal proceedings is to obtain reliable knowledge about the event of a criminal offense and the guilt of the accused (Law № 2341-III, 2001).

Proof is of criminal and criminal procedural essence. Criminal essence implies that during the process of proof, the fact of criminal violation or its absence is established, it is typified, as well as the principle of inevitability of legal liability is implemented. Criminal procedural essence of the proof, in its turn, supposes that the rights and legitimate interests of all parties in the criminal process are observed; issues arisen in criminal proceedings are tackled grounding only on well-attested facts established during the process of proof; involvement of parties concerned guarantees the observance of criminal process principles (competition, right to protection etc.); evidence is the basis for all procedural decisions in criminal proceedings. The process of proof is the way to reenact the real events of a crime, to study out their essence and to make appropriate procedural decisions.

This process forms a set of legal proceedings and relations, which can be grouped into separate, comparatively independent elements, which are common for all criminal proceedings (Udalova et al, 2015).

As to implementing theoretical aspects of cybercrime proving into practice, it is worth mentioning that, according to the national legislation, the investigation of the mentioned above category of crimes starts after the information about establishing the fact of such offence has been enlisted in the Uniform Registry of Pretrial Investigation, and is completed after the bill of indictment with its further referring to the trial has been issued against a guilty person, or in case the criminal proceeding has been closed. In pretrial investigation, an investigator/public prosecutor is authorized to apply all proceeding means outlined in the current CPC of Ukraine to criminally prosecute people suspected in committing cybercrimes; as well as, while carrying out overt and secret investigating (crime detecting) actions by ordering relevant expertise etc.

In investigating cybercrimes, a special attention is paid to evidence collecting. A prosecuting party collects evidence by carrying out overt and


Creative Commons Attribution 4.0 International (CC BY 4.0)

secret investigating (crime detecting) actions; reclaiming and obtaining personal items, documents, data, expertise reports, inspection and audit reports from state bodies, local self-governments, entities, establishments and organizations, officials as well as individual persons; by cooperating with international partners during criminal proceedings; by carrying out other activities set out in the CPC of Ukraine (Mulyarand & Hovpun, 2019).

The primary objective of an investigating officer at the first stage of cybercrime investigation is to study the information environment of a crime, that is, to establish the type of a computing machine (host), where the information (data) accessed in an unauthorized way was stored and processed (Web-host, personal computer, cell phone, e-credit card), which will allow to define the direction of further investigative activities; to establish the kind of the operating system (Unix, Linux, Netware, Windows) accessed in an unauthorized way, as well as the kind of software used for committing a crime, which will help significantly narrow a possible suspect pool down; to determine the hardware and software impacted by unauthorized access, and find out the means and tools used for an unauthorized access, which will enable to create an objective view of the trials of crime (Burbelo, 2013).

Cybercrimes are generally committed by well-trained, highly-intelligent people, with excellent command in computer technologies. Thus, it is essential to engage in the investigation of such crimes experts and professionals of the field, who can conduct an expert examination. An expert conclusion is considered to be a detailed description of an examination with a conclusion by those who are authorized. An authorized person is an expert with special knowledge in the field, where the expertise is carried out. Expertise is a type of evidence, thus, it is of a particular essence in the process of cybercrimes proof.

Cybercrime investigation proves it necessary to carry out overt and secret investigating (crime detecting) actions to get evidence from different sources. Questioning of a complainant, victim (if available) and witnesses is an important process to get evidence through testimony. Testimony is facts provided verbally or in a written form during the interrogation of a suspect, charged person, witness, victim, expert about the known facts, which are essential for a certain criminal proceeding (MECP, 2019).

Temporary availability of items and documents is also essential in investigating cybercrimes, as it secures criminal proceeding (in case of document seizure). It means the person possessing such items and documents allows the criminal proceeding party to examine, copy and, in case of an investigating judge's rule or court, seize them (to perform seizure). Such measure provides an opportunity to obtain items and documents which can be used as evidence, provided that their implication in a cybercrime has been proven.

It is worth mentioning that such procedural actions as inspection or search of property are appropriate while documenting cybercrimes. Their main aim is to reveal tools and means of committing a cybercrime (in particular, computer hardware) or to identify a person having committed it.

Taking into account that cybercrimes are illegal actions with high latency, in practice there are problematic issues related to the documentation process. First of all, the above is conditioned by the fact that in the vast majority of cases negative consequences occur after a certain period of time.

At the same time cybercrimes are international by nature and generally do not fall under the jurisdiction of a particular state. It means that the offender may be abroad and the object of encroachment may be located in Ukraine. There is no consensus among lawyers regarding the scene of the crime in this case. At the same time, it is necessary to take into account the provisions of part 1 of article 218 of the Criminal Code of Ukraine, according to which the pre-trial investigation is carried out by the investigator under whose jurisdiction the scene of the criminal offence is (Law № 4651-VI, 2013).

A significant problem is the process of identifying and documenting evidence since the "virtual traces" of the evidence can be changed or destroyed. Despite the fact that any actions and keystrokes on the computer are recorded on the hard drive and can be deleted by certain software systems, the physical destruction of the computer hard drive will make it impossible to retrieve them.

In investigating cybercrimes the issue of collecting evidence remains challenging for the parties. The data presented by the prosecution or defense party is mostly "virtual" in its form. In case the information is found on the computer, it must be analyzed and documented according to the established procedural form. As a rule, in such a case the hard drive is recognized as material evidence. However, due to the virtual


Creative Commons Attribution 4.0 International (CC BY 4.0)

lack of access to the array of information, the only source of evidence is the expert's conclusion based on the results of the computer-technical examination. The issue of identifying the person who committed the unlawful act is also rather questionable, since it is necessary to exclude the risk of the remote access and usage of a technical device.

In the process of documenting a cybercrime, it is reasonable to enact the entire range of covert investigative actions enshrined in the Criminal Code of Ukraine. For example: removing information from electronic information systems (Article 264 of the Criminal Code of Ukraine), documenting and storing information (Article 265 of the Criminal Code of Ukraine), monitoring a person or location (Article 269 of the Criminal Code of Ukraine), etc. (Law № 4651-VI, 2013).

In our opinion, the most comprehensive use of the powers and means of national law enforcement agencies and special services will allow the detective to conduct a highly qualified pre-trial investigation therefore documenting the illegal activities of the perpetrators or criminals.

**Conclusions**

Considering the fact that cybercrimes are characterized by latency, their detection and investigation is an process for the phase programmatic actions to implement measures provided by the criminal procedural legislation.

Undoubtedly, due to the scientific and technological progress, not only new sources of electronic evidence will appear, but entirely new categories of evidence. The scientific theory of procedural laws of proof in general and its criminal procedural part in particular, as well as forensic doctrine on the gathering, investigating and use of evidence are to be flexible enough since the need for this is uttered by the practice.

Optimized mechanism for cybercrime investigation requires establishing effective countermeasures. Proof at the stage of collecting evidence is carried out by the means of: conducting investigative measures and covert investigative actions; reclaiming and obtaining personal items, documents, data, expertise reports, inspection and audit reports from state bodies, local self-governments, entities, establishments and organizations, officials as well as individual persons; by cooperating with international partners during criminal proceedings; by carrying out other activities set out in the CPC of Ukraine

Taking into account the transnational nature of high-tech cybercrime, it is necessary to strengthen international cooperation for developing mutual approaches to recognize the specific illegal act as a crime in national legislation including the development of the universal standards and the implementation guidelines for documenting cybercrime.

**Bibliographic references**

Akhtyrska, N. (2018). Actual problems of cybercrime investigation: textbook. Way. (In Ukranian)

Aleksandrov, A. (2010). New Evidence Theory. International Association for the Advancement of Justice. Retrieved from https://bit.ly/3tSSY54. (In Ukranian)

Bolgov, V. (2015). Organizational and legal support of counteraction to criminal offenses committed with the use of information technology: scientific-practical way. National Academy of the Prosecutor's Office of Ukraine, pp. 202. Retrieved from https://bit.ly/3zMEpnk. (In Ukranian)

Burbelo, B. (2013). Forensic foundations of combating cybercrime. Current issues of cybercrime investigation: materials of the International scientific-practical conference. Retrieved from https://bit.ly/3OpcttE (In Ukranian)

Butuzov, V. (2010). The relationship between the concepts of «computer crime» and «cybercrime». Information security of man, society, state, № 1(3). Retrieved from https://bit.ly/3HNkerq (In Ukranian)

CETS (2005). Convention on Cybercrime. Retrieved from https://bit.ly/3n3nJ39 (In Ukranian)

Chernysh, R.F., Pogrebnaya, V.L., Montrin, I.I., Koval, T.V., and Paramonova, O.S. (2020). Formation and application of communication strategies through social networks: legal and organizational aspects. International Journal of Management, 11(06), 476-488. DOI: 10.34218/IJM.11.6.2020.041

Datareportal (2021) Digital 2021: global overview report. Retrieved from https://bit.ly/3OcpiYK

Glossary of cybersecurity terms (2012). For general. ed. O. Kopatin, E. Skulishin. K. P. K .: VB "Avanpost-Prim", 214 p. Retrieved from https://bit.ly/3tRgT4D (In Ukranian)

Gmirko, V. (2011). Retrospective analysis of ideas about the essence of evidence in the criminal process of Ukraine. Bulletin of the



Creative Commons Attribution 4.0 International (CC BY 4.0)

Academy of Customs Service of Ukraine, № 2, 112-119. Retrieved from https://bit.ly/3y4GIkm (In Ukranian)

ICED (2018). Interpol: Cybercrime is entering a new dimension. Retrieved from https://bit.ly/3HFta1L

IOCA (2018). Internet organized crime threat assessment 2018. Retrieved from https://bit.ly/3HGxttF

Kirbyatyev, O. (2010). Computer crimes: realities of the present, problems of struggle against them and probable ways of their decision. Bulletin of Zaporizhia National University, № 1. S. 165–170. Retrieved from https://bit.ly/3NbaZ58 (In Ukranian)

Komarova, L.A., Kaluhina, T.V., Pohoretskyi, M.A., Hribov, M.L., & Cherniak, A.M. (2020) Formation of Communication Innovations in the Development of the Territorial Telecommunications Complex. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(3), pp. 385-388. DOI: 10.35940/ijitee.B7589.019320. Retrieved from https://bit.ly/3y5YcwO

Kostenko, S. O., Strilchuk, V. A., Chernysh, R. F., Buchynska, A. J., & Fedoronchuk, A. V. (2021). Legal aspects of the cryptoassets market and its possible threats to the national security of Ukraine and Poland. Amazonia Investiga, 10(41), 53-64. https://doi.org/10.34069/AI/2021.41.05.5

Kravtsova, M. (2015). The concept of cybercrime and its features. Journal of Kyiv University of Law, № 2, pp. 320–324. Retrieved from https://bit.ly/3HJCC4f (In Ukranian)

Law № 2341-III. Criminal Code of Ukraine. Information of the Verkhovna Rada of Ukraine. № 25-26, 2001. Retrieved from https://bit.ly/3OcXYJV (In Ukranian)

Law № 2824-IV. On ratification of the Convention on Cybercrime, Information of the Verkhovna Rada of Ukraine, 2005. Retrieved from https://bit.ly/3n5sSYH (In Ukranian)

Law № 4651-VI. Criminal Procedure Code of Ukraine. Information of the Verkhovna Rada of Ukraine, 2003. Retrieved from https://bit.ly/3zS8UrP (In Ukranian)

Loboyko, L. (2005). Criminal procedural law: a course of lectures. Manual, pp. 456. (In Ukranian)

MECP (2019). Samples and forms of procedural documents: a practical guide-commentary, pp. 160. Retrieved from https://bit.ly/39KkniM (In Ukranian)

Mulyar, G., & Hovpun, O. (2019). Features of proving cybercrimes. Right. Man. Environment, № 3. pp. 135-136. (In Ukranian)

Order № 157. On approval of Typologies of legalization (laundering) of proceeds from crime in 2013. Order of the State Financial Monitoring Service of Ukraine, dated 25.12.2013. Retrieved from https://bit.ly/3QCgo8f (In Ukranian)

Pohoretskyi, M. (2004). Conceptual approaches to the fight against crime and protection of human rights in foreign countries. Problems of legality, № 68. pp. 122–131. (In Ukranian)

Pohoretskyi, M. (2007). Functional purpose of operational and investigative activities in criminal proceedings. Monograph, pp. 505. (In Ukranian)

Pohoretskyi, M. (2012). Cybercrime: to define the concept. Bulletin of the prosecutor's office, № 8. pp. 89–96. (In Ukranian)

Pohoretskyi, M. (2015). A new concept of criminal procedural evidence. Bulletin of criminal proceedings, № 3, pp. 64. (In Ukranian)

Ponomarenko, A., Havryliuk, L., Anheleniuk, A.M., & Drozd, V. (2020). Inadmissibility of Evidence in Criminal Proceedings in Ukraine. Amazonia Investiga, 9(29), 147-155. https://doi.org/10.34069/AI/2020.29.05.17

Shumylo, M. (2013). The concept of «evidence» in the Criminal Procedure Code of Ukraine: an attempt to critically reconsider the ideology of the normative model. Visnyk of the Supreme Court of Ukraine, № 2 (150), pp. 40-48. Retrieved from https://bit.ly/3OncjmQ (In Ukranian)

Sibilova, N. (1990). Admissibility of evidence in the Soviet criminal process. K: NMK VO, pp. 216. (In Ukranian)

Stakhivsky, S. (2005). Theory and practice of criminal-procedural evidence: monograph. K: NAVS, pp. 272. (In Ukranian)

Sviatun, O., Goncharuk, O., Chernysh, R., Kuzmenko, O., & Kozych, I. (2021). Combating cybercrime: economic and legal aspects. WSEAS Transactions on Business and Economics, 18, pp. 751-762. https://doi.org/10.37394/23207.2021.18.72

Onyshchuk, S.V., Onyshchuk, I.I., Petroye, O., & Chernysh, R. (2020). Financial Stability and its Impact on National Security State: Organizational and Legal Aspects. International Journal of Economics and Business Administration, Vol VIII, Issue 1, pp. 353-365. https://doi.org/10.35808/ijeba/429



Creative Commons Attribution 4.0 International (CC BY 4.0)

Udalova, L., Pismenny, D., Azarov, Y., and others (2015). Theory of forensic evidence in questions and answers Tutorial. Primary literature publishing center, pp. 104. Retrieved from https://bit.ly/3zSy5KP (In Ukranian)

Vasylkovsky, I. (2018). The concept of «cybercrime» and «cybercrime»: status and relationship. International Legal Bulletin: current issues (theory and practice), Issue 1-2 (10-11). pp. 276 - 282 Retrieved from https://bit.ly/3QDtrX6

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? Int. Cybersecur. Law Rev, 1, pp. 63-72, https://doi.org/10.1365/s43439-020-00012-5



Creative Commons Attribution 4.0 International (CC BY 4.0)