Genesis and issues of using latest technologies and artificial intelligence in criminalistics, forensic expert activity and pre-trial investigation

Oleksandr Ukhno *
* Doctor of Law, Professor, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0002-4771-0531, e-mail: u-kafedra@ukr.net

DOI: 10.32353/khrife.3.2021.04 UDC 343.98
Submitted: 8 Nov 2021 / Reviewed: 9 Nov 2021 / Approved for Print: 15 Nov 2021 /
Avialable online: 30 Dec 2021

The genesis of development and ways to improve theoretical and applied areas of criminalistics, forensic expertology and criminal procedure for solving forensic, procedural, organizational and other issues of implementation and use of science and technology in pre-trial investigation and trial of criminal offenses in various historical offenses in Ukraine. Special attention is paid to the scientific approach to the selection, implementation, use of computers, telecommunications, digital and other modern technologies and networks, artificial intelligence and advances in science and technology in forensics, expertise and pre-trial investigation. The scientific positions of individual scientists and representatives of domestic and foreign scientific schools on these issues were studied and analyzed (in particular, on the discussion, coverage and legislative consolidation in the legal and procedural mechanisms of selection, implementation and use of these technologies). The author's vision is expressed and the scientific position on the raised problem questions and ways of their decision is formulated.

The aim is to analyze the historical development and current state of forensic, procedural and organizational issues of selection, licensing, use, adaptation of modern information, digital, telecommunications, computer and other technologies (including artificial intelligence) in forensics, expertise and pre-trial investigation, as well as the regulatory framework governing certain issues in this area.

This article is translation of the original Ukrainian content, which source is available at the link: *https://khrife-journal.org/index.php/journal* (translation by Andriy Bublikov). The author acknowledges translation as corresponding to the original.

Keywords: *criminalistics; forensic expert activity; pre-trial investigation; modern technologies; computer networks; informational space; digital technologies; artificial intelligence; selection; adaptation.*

Research Problem Formulation

Human being is constantly evolving, trying to adapt to his needs the world around. In the beginning of its existence it learned to use wood and stones for its survival, and today it has reached such a scientific level that it is able to master even outer space. Human of the XXI century can no longer imagine his existence without the latest means of communication, which he is improving day by day. Those who try to live at the expense of others and commit criminal offenses cannot imagine their lives without it. All over the world, law enforcement agencies oppose the activities of such individuals to the latest advances in science and technology, applying modern scientific approaches to the selection, licensing, implementation and adaptation of innovations in methods of investigating negative phenomena. This fully applies to the application of the latest advances in science and technology in the field of information, telecommunications, computer, digital and other technologies, artificial intelligence in crime counteraction, in particular in forensic science and pre-trial investigation.

Future development, formation and use of forensic knowledge are determined by scientific and technological progress. Thus, we share the opinion of famous criminologist V. Yu. Shepitko that creation of information social environment contributed to technologization of criminalistics, development and implementation of information, telecommunications, digital and other modern technologies and artificial intelligence. In new conditions, criminalistics moves from traditional study of materially fixed traces to the study of sound, electronic or genomic traces. The methods, techniques and methods of working with such traces, the rules of their collection, research and recording are also changing[1]. Crime commission of s in the field of modern information and other technologies acquires an international, transnational character, in addition, victims of such crimes and the perpetrators themselves may be in different countries (for example, crimes in prisons). For combating such crimes, it is especially important to strengthen and improve international cooperation in this area, increase its effectiveness. Currently, international organizations and authorities of many countries are actively taking organizational and legal measures to prevent and combat crime in the field of modern information and other technologies. For this purpose, the codifier of the General Secretariat of Interpol separately providing for computer crimes, has been developed on the basis of the system of forensic classification of methods of committing offenses in

1 Шепітько В. Ю. Роль професора М. В. Салтевського у формуванні методологічних засад криміналістики. Актуальні питання судової експертизи та криміналістики : зб. мат-лів Міжнар. наук.-практ. конф. (Харків, 07—08.11.2017). Харків, 2017. С. 7—8.

the field of information technology [2]. In order to prevent crimes committed in the field of information technology, the Council of Europe signed Council of Europe's *Convention on Cybercrime* (ETS No. 185), better known in Ukraine as the *Budapest Convention* [3] (hereinafter referred to as *Convention*) on 23 November 2001 in Budapest. It is open for signature by both member states of the Council of Europe and non-member states that have participated in its development (in particular, the United States and Japan).

In addition, the European Committee on Crime Problems (CDPC) (in order to increase effectiveness of combating such crimes and the legal definition of a group of crimes related to computers and information technology in Europe) in 1990 prepared recommendations for inclusion of criminal law in European countries. norms of the *minimum list* and *optional list* of computer crimes. In early 2002, Minutes № 1 to the Convention was additionally adopted, adding to this list crimes of racist, xenophobic and other nature that incite violence, hatred or discrimination against an individual or group of persons and/or on the basis of race, nationality, religion or ethnicity. The mentioned minutes was also ratified by the Verkhovna Rada of Ukraine. According to the Convention, crimes are classified into four groups, namely: 1) directed against the confidentiality, integrity and availability of computer data and systems (illegal access (Article 2), illegal interception (Article 3), impact on computer data (unlawful intentional damage, destruction, deterioration, alteration or blocking of computer data) (Article 4) or systems (Article 5)), illegal use of special technical devices (Article 6) and software developed or adapted for commission of crimes under Art. 25, as well as passwords, access codes, their analogues, with which it possible to access computer system as a whole or any part of it (rules of Article 6 apply only if the use (distribution) of specific technical devices aimed at committing illegal acts); 2) related to use of computer means (forgery and fraud using computer technology) (Articles 7, 8): malicious and illegal input, modification, deletion or blocking of computer data that entails authentication data intended to be considered or used for legal purposes as authentic); 3) carried out for the purpose of distribution through computer systems (providing proposals for the use, distribution and acquisition of various types of child pornography, as well as availability of child pornography in computer data storage of a person; Article 9); 4) related to infringement of copyright and related rights to software (Article 10; in Ukraine: Article 176 of the Criminal Code of Ukraine [4], hereinafter referred to as Criminal Code) [5].

According to the current legislation of Ukraine, by 2021 the level of development of the information society in our country should be harmonized with the global way of integration of national and global information spaces. However, in order to

2 Операції з кіберзлочинності / Офіційний сайт Інтерполу. URL: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations (date accessed: 06.11.2021).

3 Конвенція про кіберзлочинність : ратифік. Законом України від 07.09.2005 р. № 2824-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (date accessed: 06.11.2021).

4 Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (date accessed: 06.11.2021).

5 Конвенція про кіберзлочинність ... . URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (date accessed: 06.11.2021).

fully enjoy the benefits of the information society, our country should also accept the negative consequences of such development; more modern and intensive ways (instead of traditional one) of committing criminal offenses. Therefore, we share the position of V. P. Bakhin that criminalistics should work to predict and prevent that can become a crime in the near future [6], and this applies to research and solving problems of combating crimes in the field of telecommunications, information, computer. computer, digital technologies, artificial intelligence and other latest advances in science and technology. According to the results of the analysis of the crime situation, there is a tendency for criminals to increasingly use information as an object of encroachment or a tool of criminal activity in the information environment (cyberspace) on various legal relationships: from national security to private property. The mechanism and dynamics of such crimes significantly complicate pre-trial investigations for law enforcement agencies and criminal proceedings for courts. According to statistics, in criminal proceedings during 2014—2018 there were crimes committed using high information technologies: 2014 — 4883, 2015 — 6026, 2016 — 6219, 2017 — 10 872, 2018 — 131. At the same time (against the background of an overall increase in cybercrime), the detection rate of such crimes tends to decrease annually, in particular, investigators have drawn up indictments: 2014 — 797, 2015 — 756, 2016 — 453, 2017 — 764, 2018 — 666 [7].

Investigating the criminological factors of committing crimes in cyberspace, D. Marenych found that in 2009 56 people were convicted, in 2010 — 69, in 2011 — 56, in 2012 — 80, in 2013 — 49, although registered such criminal proceedings are many times more. Among convicts, the majority of men are 90.82 %, women — 8 %, and their number is declining (for example, in 2009 their share was 21.5 %, in 2010 — 8.7 %, in 2011 — 12.5 % , 2012 — 1.25 %, 2013 — 6.1 %). The highest criminal activity is characteristic of persons aged 30 to 50 (44.92 %), aged 25 to 30 — 27.2 %, aged 16 to 18 — 0.33 %, and aged 50 to 65 — 4.91 % (therefore, hackers are not necessarily teenagers). At the same time, 44.9 % of convicts are able to work, but have not worked or studied anywhere [8]. The same trend has been observed in recent years. This indicates a lack of readiness of law enforcement agencies to counter not only the manifestations of cybercrime but traditional technically updated crime. As information, telecommunications, digital and other technologies, as well as cyberspace networks, various types of communications, artificial intelligence and other modern advances in science and technology are increasingly used for criminal purposes, the need to select, apply and adapt all these tools is urgent. to the needs of criminology, expertise and pre-trial investigation, namely the development of appropriate methods of investigation, which would involve the use of common methods, tools and techniques to solve typical problems of pre-trial investigation

6 Бахин В. П. Криминалистика. Проблемы и мнения (1962—2002). Киев, 2002. С. 15.

7 Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія ; за заг. ред. А. Ф. Волобуєва. Одеса, 2020. С. 5.

8 Маренич Д. Соціально-демографічні ознаки особи, що вчинила злочин у сфері використання ЕОМ, систем, комп'ютерних мереж, мереж електрозв'язку. Вісник прокуратури. 2014. № 9. С. 91—97.

at different stages [9], that prompted to choose this topic.

Analysis of Essential Researches and Publications

Similar issues were studied by: O. V. Baulin, F. Yu. Berdychevskyi, A. S. Bilousov, L. V. Borisov, V. M. Butuzov, V. B. Vekhov, V. O. Golubov, I. M Gutkin, O. Yu. Dovzhenko, A. Ya. Dubinskyi, V. V. Zhuravel, R. A. Kalyuzhnyi, L. M. Karneev, M. V. Karchevskyi, O. M. Kliuiev, O. O. Knyzhenko, M. O. Kravtsova, V. A. Korshenko, O. M. Larin, D. Marenych, O. A. Samoilenko, E. B. Simakova-Yefremian, D. P. Pysmennyi, I. V. Pyrih, V. O. Prikhodko, M. A. Pogoretskyi, V. M. Tertyshnyk, V. Yu. Shepitko, V. P. Shelomtsev, O. M. Yurchenko, O. O. Yukhno [10] and others. Let us consider in more detail some dissertations in which the raised questions are investigated. Thus, the issue of criminological characteristics of cybercrime and its prevention by law enforcement agencies was studied in 2016 by M. O. Kravtsova; theoretical and methodological bases of forensic telecommunication examination in 2017 were considered by V. A. Korshenko; O. A. Samoilenko and O. Yu. Dovzhenko devoted their research papers to the issues of methodology basics of investigating crimes committed in cyberspace in 2020. Special attention should be paid to other researches which results are presented in next research papers: *Combating Cybercrime in Ukraine* and *Management of Fight against Crime in High Technology* by V. M. Butuzov, *Prevention Crimes in the Field of High Technology: Look into the Future* by Yu. M. Yurchenko, *Crimes in the use of computers, computer networks and telecommunications networks committed by organized criminal groups and criminal organizations: problems of qualification and prevention* by M. V. Karchevskyi.

However, solution genesis of forensic, procedural and organizational issues concerning the application of modern telecommunication, information, computer and digital technologies in

9 Самойленко О. А. Op. cit.

10 Клюєв О. М. Удосконалення експертного забезпечення правосуддя: теоретичні, правові та організаційні аспекти. Теорія та практика судової експертизи і криміналістики : зб. наук. пр. 2019. Вип. 19. С. 102—117. DOI: 10.32353/khrife.1.2019.08 (date accessed: 06.11.2021) ; Шепітько М. В. Проблеми виявлення та розслідування злочинів проти правосуддя, що вчиняються професійними учасниками судочинства (провадження). Ibid. С. 48—57. DOI: 10.32353/khrife.1.2019.04 (date accessed: 06.11.2021) ; Шепітько В. Ю., Авдєєва Г. К. Проблеми застосування науково-технічних засобів та інноваційних продуктів у діяльності органів правопорядку. Ibid. Вип. 20. С. 11—26. DOI: 10.32353/khrife.2.2019.01 (date accessed: 06.11.2021) ; Хараберюш І. Ф. Окремі погляди щодо співвідношення спеціальної техніки правоохоронних органів та криміналістичної техніки. Ibid. С. 88—102. DOI: 10.32353/khrife.2.2019.06 (date accessed: 06.11.2021) ; Філіпенко Н. Є., Снігерьов О. П., Бубліков А. В. Застосування спеціальних знань під час виявлення, профілактики й розслідування злочинів у сфері комп'ютерної інформації та високих технологій (оглядова стаття). Ibid. 2020. Вип. 22. С. 162—178. DOI: 10.32353/khrife.2.2020.12 (date accessed: 06.11.2021) ; Пиріг І. В., Приходько В. О. Криміналістичні обліки: проблеми класифікації. Ibid. 2021. Вип. 23. С. 45—60. DOI: 10.32353/khrife.1.2021.03 (date accessed: 06.11.2021) ; Сімакова-Єфремян Е. Б. Впровадження новітніх методів експертних досліджень та підходів до здійснення судово-експертної діяльності — необхідний фактор експертного забезпечення правосуддя. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : мат-ли міжнар. «кругл. столу» (Харків, 12.12.2019). Харків, 2019. С. 123—128 та ін.

criminalistics and pre-trial investigation has not been comprehensively studied recently.

Given rapid development of latest information and other technologies mentioned above, some theoretical and law enforcement forensic, organizational, operational and investigative and procedural use specifics of such technologies and networks in criminalistics, forensic expertology, pre-trial investigation require further comprehensive and conceptual research. At the same time, issues of combating latency with such types of crimes remain unresolved, as latency can be minimized, in particular, by influencing the perpetrators of such crimes. Therefore, importance of research on forensic characteristics and criminological portrait of the offender and the solution of other urgent issues that will determine the direction of further research.

Within framework of this research article we will try to investigate the issues raised and suggest ways to solve certain issues(in particular, the selection, licensing, implementation, adaptation and use of the latest advances in science and technology). Deficiencies in theory and practice, as well as the lack of timing of selection, licensing, testing and implementation of modern advances in science and technology in criminology, expertise and law enforcement pre-trial investigation to some extent reduce the effectiveness of detection, detection and investigation of criminal offenses. (investigative) actions and covert investigative (investigative) actions by investigation, inquiry, prosecutor's office, operational units, which negatively affects the timeliness and quality of pre-trial investigation and trial in general and the development of appropriate methods of investigating criminal offenses in particular.

Research Paper Purpose

The purpose is an analysis of the historical development and current state of forensic, procedural and organizational issues of selection, licensing, use, adaptation of up to date information, digital, telecommunications, computer and other technologies (including artificial intelligence) in forensics, expertise and pre-trial investigation, as well as the regulatory framework governing certain issues in this area.

Main task is to make proposals and recommendations on ways to solve the identified problems at the theoretical, law enforcement and legislative levels.

Academic research novelty. Scientific research has the following elements of novelty: *first* it was carried out at the intersection of criminalistics, expertology, criminal law and process; analyzed the historical development and current state of selection, licensing, implementation and use of scientific and technical achievements (in particular, in the field of information, telecommunications, computer, digital and other technologies, tools and networks), as well as developing appropriate investigative methods; improved proposals and recommendations for solving existing issues through radical changes in the scientific research of criminalistics, expertology and pre-trial investigation with the use of innovations.

Main Content Presentation

Rapid and dynamic information development, telecommunications, computer, digital and other technologies, artificial intelligence is increasingly changing economic aspects, political and social life around the world. In the mid-1950s, not every family had a TV, a PC in the mid-1970s, and nowadays no one will

be surprised by an individual smartphone. According to *Nua Internet Surveys*, the number of Internet users has increased from 80,000 (1988) to 4.5 billion (2020) and continues to grow. Since the entry into force of the Criminal Procedural Code of Ukraine , every personal computer of the investigator that is searched in the Unified Register of Pre-Trial Investigations has an Internet connection providing law enforcement officers a number of modern information tools for registration of applications and notifications of criminal offenses and conducting investigative actions and covert investigative measures. Increase in the number of PCs and Internet users, mobiles and their varieties affects the number of crimes committed using modern information technology. This is evidenced by statistics: in Ukraine, 217 such crimes were registered in 2016 and 6,000 in 2018 and then their annual growth was over 25 %, given the significant latency and imperfection of current legislation etc. In this regard, the system of the Ministry of Internal Affairs of Ukraine has created special units to combat cybercrime, developing appropriate methods and practices in this area of organizational, investigative, operational and investigative and other activities. It is no coincidence that in 1992 the UN added the following types of crimes to the list of transnational organizations, equating to: illegal money laundering; terrorist activities; organized drug trafficking; theft of works of art, intellectual property; illicit trafficking in arms, human beings and human organs; seizure of aircraft and land transport; maritime piracy; fraud; environmental crimes. If currently different social groups and different age groups use the above and other latest technologies (especially the Internet) and such use is becoming more active day by day, then in the activities of law enforcement agencies (including police) due to limited funding, selection of such technologies, their application, adaptation and resolution of licensing issues are rather slow.

Pursuant to recommendations of international institutions and international legal acts, domestic lawmakers have criminalized crimes in the use of computers and computers, systems and computer networks and telecommunications networks in Ukraine. The generic object of crimes, the responsibility for which is determined by section XVI: *Criminal offenses in the use of electronic computers (PCs), systems and computer networks and telecommunication networks* of the Criminal Code of Ukraine [11] is a set of relations arising from the processing (collection, input, recording, conversion, reading), storage, destruction, registration), protection of computer information and operation of computers, computers, automated systems, computer networks or telecommunication networks. The subject of crimes for which liability is provided in Sec. XVI of the Criminal Code of Ukraine, can be: 1) computers (PCs); 2) automated systems; 3) computer networks; 4) telecommunication networks; 5) information; 6) software or hardware; 7) telecommunication messages. It should be noted that section XVI: of the Criminal Code of Ukraine is characterized by inconsistency of terms (both in section itself and in relation to other regulations) and the *computer (PC)* term is any device or group of interconnected devices, one or more of which, according to a certain program, automatically processes information and is equipped with auxiliary equipment (device) that allows to change or overwrite management programs and/or data needed to implement the CPU

11 Кримінальний кодекс України ... . URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (date accessed: 06.11.2021).

target functions) in general nowadays is already archaic. Optical, quantum, and biocomputers exist that means computers based on non-electronic technologies, so the term computer is a definition that will soon be used (in the case of computer criminals using new neurocomputers and/or artificial intelligence) will no longer allow the criminalization of illegal acts. According to Art. 1 of the Law of Ukraine: *On Information Protection in Telecommunication Systems* information (automated) system is an organizational and technical system where information processing technology using hardware and software is implemented [12]. As it is known, a computer network is a complex (set) of computers connected by communication lines. Depending on the speed of data exchange between work computers and the size of the area covered, there are local, regional and global computer networks. Given the provisions of Art. 1 of the Law of Ukraine: *On Telecommunications*[13], it is possible to conclude that telecommunication networks is a set of technical means of telecommunications and facilities designed for routing, switching, transmission and or reception of signs, signals, written text, images and sounds or messages of any kind by radio, wired, optical or other electromagnetic systems between the terminal equipment.

The cooperation of criminalists, mathematicians, physicists and representatives of other branches of science in the development of cybernetic research methods has contributed to the introduction of modern technical advances in forensic practice. In particular, computer technology today is an indispensable effective tool for modern investigators, researchers, experts, prosecutors, judges and others. and the main way to improve such work[14]. Thereby there is an urgent need to study the genesis of solving forensic, procedural and organizational issues in the use of information, telecommunications, computer and digital technologies in theory, law enforcement and forensic science and criminal procedure, as well as their trends and scientific experience. further improvement and resolution of the issues raised in this article.

As early as 1969, L. Yu. Arotsker noted that for practical use of computers in expert activities and practice it is necessary to develop algorithms and modes of their operation that would ensure sufficient reliability of answers for identification tasks and the correct solution of both organizational and procedural issues, without which further use of computers in the activities of forensic experts is impossible[15]. Discussing this, R. M. Lanzman noted that priority solution needs to be organizational and procedural issues (in particular, at what stage of scientific and experimental verification of computer reliability they can be used for forensic examinations). According to him, literature of 1968 already contained

12 Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (date accessed: 06.11.2021).

13 Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text (date accessed: 06.11.2021).

14 Іванов В. Г., Іванов С. М., Карасюк В. В. та ін. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. ; за заг. ред. В. Г. Іванова. 4-те вид., змін. і доп. 2014. С. 4.

15 Ароцкер Л. Е. Организационные и процессуальные вопросы использования электронно-вычислительных машин в экспертной практике. Криминалистика и судебная экспертиза. 1969. Вып. 6. С. 182—183.

descriptions of the use of computers while conducting forensic examinations, however, then correct recognition was not achieved in all cases and areas [16].

An important condition for the use of computers in expert practice is lack of gross errors in operation of the computer for each of tested algorithms. If certain types of modern technical means, working according to a certain algorithm, experimentally and in a sufficient number of experiments give the correct answers, then such an algorithm can also be used during forensic examinations. Otherwise, there are always doubts about the reliability of the algorithm chosen by the expert. At one time, when the scientific community had just raised these issues, M. S. Strohovych noted that use of investigative, expert and legal practice of new techniques and tools developed by technical and natural sciences, can only be thoroughly tested. and their tools are able to provide reliable results [17].

Using modern technical advances and computers for research on physical evidence, a forensic expert should find out the mechanism of research activities of a particular newly created technical device, understand signs and mechanisms of recognition, issue solving and decision making. Without this, forensic expert has no right to use such latest scientific advances, technology, etc., as well as give an opinion to the investigator, coroner, prosecutor, investigating judge, trial, because conditions and nature of the procedural activities of these persons do not involve research methods. methods. Certainly, the belief in absolute objectivity of computers and other scientific achievements and at the same time lack of understanding of the mechanism of their activities, the signs they operate, does not provide forensic expert with right to use computers and other scientific achievements while forensic examination. References to the possibility of using computers in other areas of human activity, even if you do not know the mechanism of their work, in law enforcement do not work, because in it (in particular, in legal research), unlike any other activity, every fact should be proven and justified.

According to L. H. Edzhubova, different types of tasks of forensic research involve development of various algorithms, each of which should solve a specific forensic task. It is impossible to develop a single universal algorithm for research on all objects, even one species of examination. In this regard, there is a need to develop and implement in forensic expert activities and investigative and legal practice systems of different algorithms designed to solve a specific class of problems[18] that is relevant to this day. He stated that such an approach at that time (1968) was most often used to conduct forensic handwriting examinations.

The need for several algorithms will continue to exist for developing and improving cybernetic methods of many types of forensic examinations, that will allow to solve one investigative task using several algorithms, as unambiguous results obtained using different algorithms are more convincing.

16 Ароцкер Л. Е., Ланцман Р. М. Кибернетика и криминалистическая экспертиза почерка. Москва, 1968. С. 51, 83—85.

17 Строгович М. С. Курс советского уголовного процесса. В 2 т. Т. 1. Основные положения науки советского уголовного процесса. Москва, 1968. С. 83.

18 Эджубов Л. Г. Актуальные вопросы использования электронных цифровых вычислительных машин в судебном почерковедении. *Проблемы правовой кибернетики* : мат-лы симп. Москва, 1968. С. 167—168.

Opinion of contemporary scientists on the need for constant selection, application and adaptation of the latest advances in science and technology in expert activities in certain areas is valid to this day. For example, identification of fingerprints while fingerprinting by computer (PCs) significantly speeds up the procedure, in contrast to processing of forensic records of fingerprints manually by employees of expert institutions. Modern drones (unmanned aerial vehicles and ground and submarine drones) are controlled by special personal computers while scene inspection when the objects of crime or parts of the bodies of the victims are at a certain distance from the main scene or when they are used for detention criminals, etc. For counteracting the explosion threat at the scene, forensic laboratories use robotics to identify an explosive device. Actively use computer equipment and networks in law enforcement, and free access to relevant forensic and other records will allow investigators, investigators, operatives to significantly accelerate the priority investigative (search) actions (for example, to identify the offender whose genomic traces are found on scene). It is promising to replenish forensic records with such new types as: fixation of the iris, video computer recognition of the face by image, torso X-ray film, genomic portraits, etc.

Use of modern advances in science and technology makes it possible to expand the range of issues that can be solved by experts. Thus, in the case of investigations of crimes in the use of computers, computers, systems and computer networks and telecommunications networks, conduct as traditional forensic (trace evidence, handwriting, substances and materials, etc.), economic, forensic accounting , and special for this composition of crimes computer and technical examinations. According to the tasks and specifics of the objects of research today, the following subtypes of examination can be distinguished within this type: 1) technical computers and peripherals; 2) technical equipment for protection of computer information; 3) machine data used in a computer network[19]. Methodical bases of forensic telecommunication examination that was successfully implemented in the activity of expert institutions of Ukraine, in 2017 were laid by V. A. Korshenko. In particular, he defined that forensic *telecommunication* examination is a kind of forensic engineering that involves forensic research based on specific expertise of telecommunication systems, facilities, networks, their components and information they transmit, receive and process, containing information about case circumstances while pre-trial investigation or trial. He argued that the generic object of this examination are material objects, their totality or parts that by their characteristics could or under certain conditions can transmit, emit and/or receive signs, signals, text, images, sounds, messages and other information using radio, wired, optical, electromagnetic and other systems, as well as software and information contained in these objects [20].

In order to investigate (Article 2 of the Criminal Procedural Code of Ukraine) cybercrime fully, quickly and impartially, to choose certain tactics and methods of investigation investigator, investigator, prosecutor, judge should know the forensic characteristics of such tactics and methods. Scientific discussions on

19 Панов М. І., Шепітько В. Ю., Коновалова В. О. Настільна книга слідчого. 3-тє вид., перероб. і допов. Київ, 2011. С. 536—537.

20 Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи : автореф. дис. ... канд. юрид. наук. Харків, 2017. С. 12—15.

this continue to nowadays. Therefore, we consider it appropriate to dwell on the forensic characteristics of information and cybercrime that contains the following elements: the offender identity, victim identity, criminal encroachment subject, crime means, trace picture.

O. H. Volevodz and D. Marenych note that offender personality is often characterized by active life position, sophistication, cunning, original and unusual thinking and behavior, caution, attentiveness, vigilance, some talent for anticipation in the preparation and commission of the crime, as well as certain post-criminal behavior and disguise. From psychophysiological point of view, he is a bright, thinking and creative person, an expert in his field, capable of technical challenges, a desirable student and / or employee. However, such a person is afraid of losing his authority or social protection within a social group or is afraid of ridicule. His behavior outwardly often corresponds to generally accepted social norms in society. According to investigative and judicial practice, computer criminals generally do not have a criminal record, and those who are already in prisons try to acquire knowledge in this area and use it in the presence of corrupt connections with the administration of correctional facilities. criminal offenses, directing them outside the places of detention. According to scientists, a significant part of such crimes are committed individually but recently there has been a tendency to complicity in group encroachments[21]. In identifying such crimes, account should be taken of their possible employment relationship with the victim organization, their behavior at work, types of technical positions held by offenders at the offense time , group to be inspected, methods of preparation, commission and concealment. crimes, as well as person age, motive and purpose of criminal acts, scope of criminal activity (hackers, crackers, etc.), financial and technical capabilities, uniqueness of computer knowledge, etc., schemes of different groups of criminals, single hackers, joint hacker group, competitor, representatives of various departments of the departmental, interdepartmental level), the characteristics of the offender, depending on the type of computer crime, etc.

The next element of the forensic characterization of these types of crimes is victim identity. According to the current Criminal Procedural Code of Ukraine of Ukraine and statistical data, victim can be both individuals and legal entities. Most of the victims are legal entities (enterprises of all forms of ownership, institutions, agencies, organizations). Given the ownership computer system, legal literature distinguishes three groups of victims of these types of crimes: owners of computer systems — 79%; customers of such owners of computer systems — 13%; third parties — 8%. The main elements of the forensic characterization of computer crimes differ in the variety of ways to prepare, commit and conceal criminal offenses, which are characterized by computer objects, methods of commission, a specific virtual trace image displayed on hardware, software or information elements of computer or other similar objects, as well as the identity of the offender and the victim. The commission of such crimes is connected with the use of various carriers of computer, telecommunication or other information of various origins, in particular: computer

21 Волеводз А. Г. Следы преступлений, совершенных в компьтерных сетях. *Российский следователь.* 2002. № 1. С. 4—12 ; Маренич Д. Криміналістична характеристика кіберзлочинів. *Вісник прокуратури.* 2014. № 12. С. 113—120.

memory, telecommunication lines, printing of materials, etc. According to A. S. Bilousov, to work with such objects requires a variety of technical tools, skills and specific expertise [22].

Another important element of the forensic characterization of such types of crimes are the methods of their commission, which include acts of conduct and actions of the offender, aimed at preparing, committing and concealing a criminal offense. The preparatory stage of committing cybercrime or other information crimes is determined by a whole system of methods, including: interception of information, obtaining unauthorized access to computer or other information, telecommunications and other equipment; manipulation of computer data and computer control commands; copying and duplication; overcoming software protection. Ways of concealing crimes are determined by the ways in which they are committed. Several classifications of methods of committing cybercrimes have been proposed in forensic readings. According to V. M. Butuzov, V. M. Gavlovskyi, L. P. Skalozub, depending on how the access to computer or other information is made, the following ways of committing the investigated crimes are distinguished: 1) direct access which information is blocked, modified, copied, and destroyed; 2) indirect (remote) access to computer or other information, carried out at a distance from another computer via a computer network; 3) mixed methods, implemented both by direct and remote access[23]. It should be noted that the elements of forensic characterization include the subject of criminal encroachment, in particular: information, funds, personal data, which in general also determine the different ways of committing such types of criminal offenses. Depending on the subject of criminal encroachment, the following groups of ways of committing the investigated crimes are distinguished: 1) information ones: illegal ways of obtaining information, in particular by unauthorized access to computers and networks, dissemination of false information; 2) financial ones: they are sometimes defined as *breaking* of banking security systems, receiving free telephone services, stealing credit cards, creating electronic pyramids, fraud in the form of remote sales or work, etc.; 3) those that harm the health and endanger the lives of people (disabling medical equipment, person terrorizing, etc.).

The last and essential element of forensic characterization of such crimes is their trace picture. It demonstrates how the offender got to the crime scene and how he disappeared from there, overcame obstacles, used his official position, achieved the criminal goal set before him (and accomplices), applied knowledge and skills, or tried to hide traces of his criminal actions. Also important for investigation and inquiry are the traces that indicating nature of the criminal's connection with the object of criminal encroachment, etc. It should be noted that in criminalistics the trace picture of cybercrime is defined as a set of information about typical traces as signs and conditions of committing a criminal offense that are characteristic of certain ways of illegal interference

22 Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. … канд. юрид. наук. Київ, 2008. С. 19.

23 Бутузов В. М., Гавловський В. Д., Скалозуб Л. П. та ін. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : навч. посіб. ; за заг. ред. Л. П. Скалозуба, І. В. Бондаренка. Київ, 2010. С. 59—62.

in computers, computer networks and correlated dependence on the identity of the offender and the object of encroachment. Traces of cybercrime can be material (in particular, manuscripts, printouts, etc.) and indicate preparation for the crime and the crime itself. Material traces can remain on computers (fingerprints, microparticles on keyboards, disk drives, printers, etc.), as well as on magnetic media and optical disks. In addition, there are traces of information that are formed as a result of exposure to computer information (by destruction, distortion). First of all, they are left on magnetic media, they are associated with changes that have occurred in the information itself compared to the initial state. Information traces also include the effects of anti-virus and test programs that can be detected by studying computer hardware, programmers' work records, anti-virus programs, and software protocols. In order to identify such traces, it is advisable to involve a specialist in computer hardware and software [24]. Participating in research on cybercrime laws, V. O. Meshcheriakov notes that analysis of peculiarities of formation of the trace picture of such crimes requires the concept introduction of "virtual traces" (as an intermediate between material and ideal traces) [25]. Criminalists not only supported his scientific position, but also developed it. Thus, O. H. Volevodz states that, given peculiarities of virtual traces, they cannot be removed, but only copied using various software and hardware [26]. It should be noted that virtual traces exist objectively on tangible media, but are not available for direct perception. It is necessary to use software and hardware to perceive them. Availability of such traces on the material carrier brings this group closer to the material traces, but does not confirm them as such. At the same time, we should emphasize that virtual traces (due to the nature of their existence), obtained from a material medium and perceived internally are not reliable, and therefore they can be misread. For example, using software and hardware, such traces are easy to forge or lose. They are similar to ideal, but they cannot be equated with ideal, because virtual traces are stored in perfect form, however, not in human memory, but in machine memory and on tangible media of machine information, they are detected using technical means and certain algorithms. The appearance of traces on physical level is caused by natural influence of computer hardware: the passage of electric current, magnetization or demagnetization of certain parts of the magnetic medium as a result of the actions of the offender. Such traces are invisible, there are no external manifestations on the hardware elements of computer objects. They can be detected, recorded, deleted and investigated only with of hardware and software use [27].

One of achievements of the scientific and technological revolution of the XXI century. There is development of artificial intelligence and robotics, but there is a lack of effective legal regulatory mechanisms in this area. In addition, there is a trend not

24 Панченко В. М. Сучасний стан та проблеми боротьби з Інтернет-злочинністю. *Боротьба з Інтернет-злочинністю :* мат-ли Міжнар. наук.-практ. конф. (Донецьк, 12—13.06.2013). Донецьк, 2013. С. 8 ; Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. … канд. юрид. наук. Київ, 2005. С. 18.

25 Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. … канд. юрид. наук. Воронеж, 2001. С. 21.

26 Волеводз А. Г. Op. cit.

27 Шепітько В. Ю. Op. cit. С. 8.

so much the impact of law on this industry, as the impact of digital technology on law. Currently, the use of artificial intelligence in criminalistics and forensic science is quite relevant and promising. Developed countries of the world consider artificial intelligence as one of the most important strategies to increase competitiveness and ensure national security. According to O. A. Telychko and co-authors, artificial intelligence is widely used in education, health care, pensions, environmental protection, public administration and law enforcement. Artificial intelligence is becoming the most important factor in the development of the digital economy of any country, but the possible threats from its use raise questions and require legal guarantees for the safe operation of its systems. There is the issue of forming the conceptual apparatus of artificial intelligence as a factor in regulating any new area [28]. For this issue resolving, the Cabinet of Ministers of Ukraine of 02.12.2020 approved the Concept of Artificial Intelligence in Ukraine [29] and the Cabinet of Ministers of 09.09.2020 approved the Government's Priority Action Plan for 2020 on these issues [30].

Thus, according to research, selection, use, adaptation of advances in science and technology in criminology, forensic science and pre-trial investigation at all historical stages have been actively supported and are supported today by scientists and law enforcement agencies. We share the right opinion of N. I. Klymenko that the knowledge of investigators and experts is valuable only when they are applied in practice [31], and we consider it expedient to extend this opinion to the direction studied here.

Conclusions

The legal basis and the state of the criminogenic situation in the country and in the world encourage further research in the use of modern advances in telecommunications, information, computer, digital technology and artificial intelligence in forensics, forensics and pre-trial investigation, as required by the current state. development of science and technology, the achievements of which are actively used by criminals to commit new types of criminal offenses. A study of the genesis of this issue has revealed that already in the twentieth century. Scientists have comprehensively studied peculiarities of using achievements of science and technology (including information,

28 Теличко О. А., Рекун В. А., Чабаненко Ю. С. Проблеми визначення та нормативного закріплення поняття «штучний інтелект» у законодавстві зарубіжних країн та України. *Юридичний науковий електронний журнал.* 2021. № 2. С. 310—313. DOI: 10.32782/2524-0374/2021-2/75 (date accessed: 06.11.2021) ; Шестак В. А., Волеводз А. Г. Современные потребности правового обеспечения искусственного интеллекта : взгляд из России. *Всероссийский криминологический журнал*. 2019. Т. 13. № 2. С. 197—206. DOI: 10.17150/2500-4255.2019.13(2).197-206 (date accessed: 06.11.2021).

29 Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження КМУ від 02.12.2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (date accessed: 06.11.2021).

30 Про затвердження плану пріоритетних дій Уряду на 2020 рік : розпорядження КМУ від 09.09.2020 р. № 1133-р. URL: https://zakon.rada.gov.ua/laws/show/1133-2020-%D1%80#Text (date accessed: 06.11.2021).

31 Клименко Н. І. Криміналістичні знання: поняття, структура, розвиток. *Криміналістика XX1 століття :* мат-ли Міжнар. наук. практ. конф. (Харків, 25—26.11.2010). Харків, 2010. С. 28.

telecommunications, computer, network, computers, communications, artificial intelligence, etc.) while pre-trial investigation and forensic examinations. Further scientific research contributed to an active discussion in this direction with unquestionable conclusions about the feasibility of further selection, licensing, testing, introduction, application and improvement of new types of science and technology in law enforcement practice. The chronology of the genesis of the use of such knowledge during forensic examinations can be determined by the order of their application (in particular, for handwriting, trace evidence, computer, telecommunications and other types of examination). The most widespread research on the use of scientific achievements of digital technologies and artificial intelligence, DNA-analysis in the theory of criminalistics and the practice of forensic expertology, investigative bodies, bodies of inquiry, prosecutors, courts. According to the genesis, the first issue of legal regulation of human-artificial intelligence in 2005 was raised by South Korean scientists, supported by their government, by enshrining doctrinal provisions, including the *Korean Robot Intelligence Act* (2005) and the *Ethical Statute of Robots*. (2007), *Legal Regulation of Autonomous Systems in South Korea* (2012)[32]. Ukrainian legislators also supported the further development, improvement and direction of development of artificial intelligence in Ukraine at the regulatory level.

In order to introduce forensic recommendations in law enforcement activities, current tasks of criminalistics are outlined, in particular: 1) formalization of forensic knowledge; 2) unification of forensic recommendations on pragmatic goals; 3) introduction of innovative developments proposed by science [33]. Given the issues raised, it is necessary to support the positions of scholars on the separation in criminology, in particular: differentiation of forensic knowledge; formation of new separate forensic theories; computerization of forensic tools and methods; expansion of the trace picture of crime, the emergence of new non-traditional traces; development of supersensitive analytical methods; the emergence of new investigative actions that are difficult or impossible to carry out without scientific and technical support; strengthening importance of scientific and technical support for the pre-trial investigation; development of new methods of investigation of crimes committed with use of scientific and technological progress advances [34].

Thus, researches on genesis and current state of application of scientific and technological achievements in criminalistics, forensic expertology and pre-trial investigation confirm the progressiveness of this area for law enforcement and criminal proceedings (Article 2 of the Criminal Procedural Code of Ukraine) to ensure and respect rights, freedoms and legitimate interests of persons in Ukraine.

32 Теличко О. А., Рекун В. А., Чабаненко Ю. С. Op. cit.

33 Шепитько В. Ю. Изменчивость криминалистики в XXI веке и ее задачи в современных условиях. *Криміналістика XXI століття :* мат-ли Міжнар. наук. практ. конф. (Харків, 25—26.11.2010). Харків, 2010. С. 58—59.

34 Тонков Е. Е., Комаров И. М. Современные тенденции развития криминалистики и судебной экспертизы. *Современное право*. 2011. № 6. С. 129—134. URL: http://dspace.bsu.edu.ru/handle/123456789/17029 (date accessed: 06.11.2021).

Генезис і проблемні питання використання новітніх технологій та штучного інтелекту в криміналістиці, експертній діяльності й досудовому розслідуванні

Олександр Юхно

Розглянуто генезис розвитку та шляхи вдосконалення теоретичних і прикладних напрямів криміналістики, судової експертології й кримінального процесу для вирішення криміналістичних, процесуальних, організаційних та інших проблемних питань запровадження й використання досягнень науки і техніки під час досудового розслідування та судового розгляду кримінальних правопорушень на різних історичних етапах розвитку цього напряму в Україні. Окремо акцентовано увагу на науковому підході до відбору, запровадження, використання електронно-обчислювальних машин, телекомунікаційних, комп'ютерних, цифрових та інших сучасних технологій і мереж, засобів зв'язку, штучного інтелекту й досягнень науки і техніки в криміналістиці, експертній діяльності й у досудовому розслідуванні. Вивчено та проаналізовано наукові позиції окремих учених і представників вітчизняних і зарубіжних наукових шкіл із названих питань (зокрема, щодо обговорення, висвітлення й законодавчого закріплення в правовому та процесуальному механізмах відбору, запровадження й використання згаданих технологій). Висловлено авторське бачення та сформовано наукову позицію щодо порушених проблемних питань і шляхів їх вирішення.

Метою є аналіз історичного розвитку й сучасного стану криміналістичних, процесуальних і організаційних проблемних питань з відбору, ліцензування, використання, адаптування сучасних інформаційних, цифрових, телекомунікаційних, комп'ютерних та інших технологій (зокрема, штучного інтелекту) у криміналістиці, експертній діяльності та досудовому розслідуванні, а також нормативно-правової бази, що регулює окремі питання цього напряму.

Ключові слова: *криміналістика; експертна діяльність; досудове розслідування; сучасні технології; комп'ютерні мережі; інформаційний простір; цифрові технології; штучний інтелект; відбір; адаптування.*

Генезис и проблемные вопросы использования новейших технологий и искусственного интеллекта в криминалистике, экспертной деятельности и досудебном расследовании

Александр Юхно

Рассмотрен генезис развития и пути совершенствования теоретических и прикладных направлений криминалистики, судебной экспертологии и уголовного процесса для решения криминалистических, процессуальных, организационных и других проблемных вопросов внедрения и использования достижений науки и техники в досудебном расследовании и судебном разбирательстве уголовных правонарушений на различных исторических этапах развития этого направления в Украине. Отдельно акцентировано внимание на научном подходе к отбору, внедрению, использованию электронно-вычислительных машин, телекоммуникационных, компьютерных, цифровых и других современных технологий и сетей, средств связи, искусственного интеллекта и достижений науки и техники в криминалистике, экспертной деятельности и в досудебном расследовании. Изучены и проанализированы научные позиции отдельных учёных и представителей отечественных и зарубежных научных школ по названным вопросам (в частности, относительно обсуждения, освещения и законодательного закрепления в правовом

и процессуальном механизмах отбора, внедрения и использования упомянутых технологий). Высказано авторское видение и сформулирована научная позиция по поднятым проблемным вопросам и путям их решения.

Целью является анализ исторического развития и современного состояния криминалистических, процессуальных и организационных проблемных вопросов по отбору, лицензированию, использованию, адаптации современных информационных, цифровых, телекоммуникационных, компьютерных и других технологий (в том числе искусственного интеллекта) в криминалистике, экспертной деятельности и досудебном расследовании, а также нормативно-правовой базы, регулирующей отдельные вопросы этого направления.

Ключевые слова: *криминалистика; экспертная деятельность; досудебное расследование; современные технологии; компьютерные сети; информационное пространство; цифровые технологии; искусственный интеллект; отбор; адаптация.*

Funding
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Disclaimer
The funders had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Contributors
The author contributed solely to the intellectual discussion underlying this paper, case-law exploration, writing and editing, and accept responsibility for the content and interpretation.

Declaration of Competing Interest
The author declares that he has no conflict of interest.

References

Arotsker, L. E. (1969). Organizatsionnye i protsessualnye voprosy ispolzovaniia ehlektronno-vychislitelnykh mashin v ehkspertnoi praktike [Organizational and Procedural Issues of PC Use in Forensic Expert Practice]. *Kriminalistika i sudebnaia ehkspertiza*. Vyp. 6 [in Russian].

Arotsker, L. E., Lantsman, R. M. (1968). *Kibernetika i kriminalisticheskaia ehkspertiza pocherka* [Cybernetics and Forensic Handwriting Examination]. Moskva [in Russian].

Bakhin, V. P. (2002). *Kriminalistika. Problemy i mneniia (1962—2002)* [Criminalistics. Issues and Opinions (1962—2002)]. Kiev [in Russian].

Bilousov, A. S. (2008). *Kryminalistychnyi analiz obiektiv kompiuternykh zlochyniv* [Forensic Analysis of Objects of Computer Crimes]: avtoref. dys. … kand. yuryd. nauk. Kyiv [in Ukrainian].

Butuzov, V. M., Havlovskyi, V. D., Skalozub, L. P. ta in. (2010). *Dokumentuvannia zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku pry provedenni doslidchoi perevirky* [Documentation of Crimes in the Field of PC Use, Systems and Computer and Telecommunication Networks while Investigation]: navch. posib. ; za zah. red. L. P. Skalozuba, I. V. Bondarenka. Kyiv [in Ukrainian].

Ehdzhubov, L. G. (1968). Aktualnye voprosy ispolzovaniia ehlektronnykh tsifrovykh vychislitelnykh mashin v sudebnom pocherkovedenii [Current issues in PC use in Forensic Handwriting]. *Problemy pravovoi kibernetiki* : mat-ly simp. Moskva [in Russian].

Filipenko, N. Ye., Sniherov, O. P., Bublikov, A. V. (2020). Zastosuvannia spetsialnykh znan pid chas vyiavlennia, profilaktyky y rozsliduvannia zlochyniv u sferi

kompiuternoi informatsii ta vysokykh tekhnolohii (ohliadova stattia) [Specific Expertise Application in Detection, Prevention and Investigation of Crimes in the Field of Computer Information and High Technology (Review Article)]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 22. DOI: 10.32353/khrife.2.2020.12 [in Ukrainian].

Ivanov, V. H., Ivanov, S. M., Karasiuk, V. V. ta in. (2014). *Pravova informatsiia ta kompiuterni tekhnolohii v yurydychnii diialnosti* [Legal Information and IT in Legal Activities]: navch. posib. ; za zah. red. V. H. Ivanova. 4-te vyd., zmin. i dop. Kharkiv [in Ukrainian].

Kharaberiush, I. F. (2019). Okremi pohliady shchodo spivvidnoshennia spetsialnoi tekhniky pravookhoronnykh orhaniv ta kryminalistychnoi tekhniky [Separate Views on Correlation between Special Equipment of Law Enforcement Agencies and Forensic Equipment]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 20. DOI: 10.32353/khrife.2.2019.06 [in Ukrainian].

Kliuiev, O. M. (2019). Udoskonalennia ekspertnoho zabezpechennia pravosuddia: teoretychni, pravovi ta orhanizatsiini aspekty [Improving Forensic Expert Support of Justice: Theoretical, Legal and Organizational Aspects]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 19. DOI: 10.32353/khrife.1.2019.08 [in Ukrainian].

Klymenko, N. I. (2010). Kryminalistychni znannia: poniattia, struktura, rozvytok [Forensic Knowledge: Concept, Structure, Development]. *Kryminalistyka XXI stolittia* : mat-ly Mizhnar. nauk. prakt. konf. (Kharkiv, 25—26.11.2010). Kharkiv [in Ukrainian].

Korshenko, V. A. (2017). *Teoretychni ta metodychni osnovy sudovoi telekomunikatsiinoi ekspertyzy* [Theoretical and Methodological Bases of Forensic Telecommunication Examination]: avtoref. dys. ... kand. yuryd. nauk. Kharkiv [in Ukrainian].

Marenych, D. (2014). Kryminalistychna kharakterystyka kiberzlochyniv [Forensic Characteristics of Cybercrime]. *Visnyk prokuratury.* № 12 [in Ukrainian].

Marenych, D. (2014). Sotsialno-demohrafichni oznaky osoby, shcho vchynyla zlochyn u sferi vykorystannia EOM, system, kompiuternykh merezh, merezh elektrozviazku [Socio-demographic Characteristics of Person who Has Committed a Crime in the Field of Use of Computers, Systems, Computer Networks, Telecommunications Networks]. *Visnyk prokuratury.* № 9 [in Ukrainian].

Meshcheriakov, V. A. (2001). *Osnovy metodiki rassledovaniia prestuplenii v sfere kompiuternoi informatsii* [Fundamentals of Methods of Investigating Crimes in the Field of Computer Information]: avtoref. dis. ... kand. iurid. nauk. Voronezh [in Russian].

Operatsii z kiberzlochynnosti [Cybercrime operations]/ Ofitsiinyi sait Interpolu. URL: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations [in Ukrainian].

Palamarchuk, L. P. (2005). *Kryminalistychne zabezpechennia rozsliduvannia nezakonnoho vtruchannia v robotu elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh* [Forensic Investigation of Illegal Interference In the Work of Computers, Systems and Computer Networks]: avtoref. dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Panchenko, V. M. (2013). Suchasnyi stan ta problemy borotby z Internet-zlochynnistiu [Current State and Issues of Combating Cybercrime]. *Borotba z Internet-zlochynnistiu* : mat-ly Mizhnar. nauk.-prakt. konf. (Donetsk, 12—13.06.2013). Donetsk [in Ukrainian].

Panov, M. I., Shepitko, V. Yu., Konovalova, V. O. (2011). *Nastilna knyha slidchoho*

[Investigator's handbook]. 3-tie vyd., pererob. i dopov. Kyiv [in Ukrainian].

Pyrih, I. V., Prykhodko, V. O. (2021). Kryminalistychni obliky: problemy klasyfikatsii [Forensic Accounting: Classification Issues]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 23. DOI: 10.32353/khrife.1.2021.03 [in Ukrainian].

Samoilenko, O. A. (2020). *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori* [Fundamentals of Methods of Investigating Crimes Committed in Cyberspace]: monohrafiia ; za zah. red. A. F. Volobuieva. Odesa [in Ukrainian].

Shepitko, M. V. (2019). Problemy vyiavlennia ta rozsliduvannia zlochyniv proty pravosuddia, shcho vchyniaiutsia profesiinymy uchasnykamy sudochynstva (provadzhennia) [Issues of Detection and Investigation of Crimes against Justice Committed by Professional Participants in the Legal Proceedings]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 19. DOI: 10.32353/khrife.1.2019.04 [in Ukrainian].

Shepitko, V. Iu. (2010). Izmenchivost kriminalistiki v XXI veke i ee zadachi v sovremennykh usloviiakh [Variability of Criminalistics in the XXI Century and its Tasks in Modern Conditions]. *Kryminalistyka XXI stolittia* : mat-ly Mizhnar. nauk. prakt. konf. (Kharkiv, 25—26.11.2010). Kharkiv [in Russian].

Shepitko, V. Yu. (2017). Rol profesora M. V. Saltevskoho u formuvanni metodolohichnykh zasad kryminalistyky [Role of M. V. Saltevskyi, Professor in Formation of Methodological Foundations of Criminalistics]. *Aktualni pytannia sudovoi ekspertyzy ta kryminalistyky* : zb. mat-liv Mizhnar. nauk.-prakt. konf. (Kharkiv, 07—08.11.2017). Kharkiv [in Ukrainian].

Shepitko, V. Yu., Avdieieva, H. K. (2019). Problemy zastosuvannia naukovo-tekhnichnykh zasobiv ta innovatsiinykh produktiv u diialnosti orhaniv pravoporiadku [Issues of Application of Scientific and Technical Means and Innovative Products in Activity of Law Enforcement Agencies]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 20. DOI: 10.32353/khrife.2.2019.01 [in Ukrainian].

Shestak, V. A., Volevodz, A. G. (2019). Sovremennye potrebnosti pravovogo obespecheniia iskusstvennogo intellekta : vzgliad iz Rossii [Modern Needs of Legal Support of Artificial Intelligence: View from Russia.]. *Vserossiiskii kriminologicheskii zhurnal.* T. 13. № 2. DOI: 10.17150/2500-4255.2019.13(2).197-206 [in Russian].

Simakova-Yefremian, E. B. (2019). Vprovadzhennia novitnikh metodiv ekspertnykh doslidzhen ta pidkhodiv do zdiisnennia sudovo-ekspertnoi diialnosti — neobkhidnyi faktor ekspertnoho zabezpechennia pravosuddia [Introduction of Latest Methods of Forensic Expert Research and Approaches to Implementation of Forensic Activities is Necessary Factor in Forensic Expert Support of Justice]. *Innovatsiini metody ta tsyfrovi tekhnolohii v kryminalistytsi, sudovii ekspertyzi ta yurydychnii praktytsi* : mat-ly mizhnar. «kruhl. stolu» (Kharkiv, 12.12.2019). Kharkiv [in Ukrainian].

Strogovich, M. S. (1968). *Kurs sovetskogo ugolovnogo protsessa* [Course of Soviet Criminal Procedure]. V 2 t. T. 1. Osnovnye polozheniia nauki sovetskogo ugolovnogo protsessa. Moskva [in Russian].

Telychko, O. A., Rekun, V. A., Chabanenko, Yu. S. (2021). Problemy vyznachennia ta normatyvnoho zakriplennia poniattia «shtuchnyi intelekt» u zakonodavstvi zarubizhnykh krain ta Ukrainy [Issues of Definition and Normative Consolidation of the Artificial Intelligence Concept in Legislation of Foreign Countries and Ukraine]. *Yurydychnyi naukovyi elektronnyi zhurnal.* № 2. DOI: 10.32782/2524-0374/2021-2/75 [in Ukrainian].

Tonkov, E. E., Komarov, I. M. (2011). Sovremennye tendentsii razvitiia kriminalistiki i sudebnoi ehkspertizy [Current Trends in Development of Criminalistics and Forensic Science]. *Sovremennoe pravo*. № 6. URL: http://dspace.bsu.edu.ru/handle/123456789/17029 [in Russian].

Volevodz, A. G. (2002). Sledy prestuplenii, sovershennykh v kompternykh setiakh [Traces of Crimes Committed on Computer Networks]. *Rossiiskii sledovatel.* № 1 [in Russian].

Ukhno, O. (2021). Genesis and issues of using latest technologies and artificial intelligence in criminalistics, forensic expert activity and pre-trial investigation. *Theory and Practice of Forensic Science and Criminalistics.* Issue 3 (25). P. 40—59. DOI: 10.32353/khrife.3.2021.04.