Open Sources of Cyberspace as Objects of Forensic Research

Mykhailo Shcherbakovskyi *

* Doctor of Law, Professor, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-1990-1231,
e-mail: shcherbakovskyi@gmail.com

DOI: 10.32353/khrife.2.2024.02 UDC 343.98
Received: 23.05.2024 / Reviewed: 24.05.2024 / Accepted for print: 26.06.2024 /
Available online: 30.06.2024

The purpose of this research paper is to use modern general and special methods of scientific cognition to investigate the procedural procedure for the formation of digital evidence based on open information from cyberspace in the context of evidence during criminal proceedings and to substantiate possibility of forensic expert research of cyberspace to obtain criminally relevant indicative and evidentiary information in the form of a conclusion an expert It is shown that computer data and electronic (digital) information are synonymous and are divided into two groups: neutral that have no significance for criminal proceedings, and criminally relevant, which contain traces of an offense and data about persons, objects, events, facts etc., which have indicative or evidential value. It has been proven that cyberspace is a separate carrier of criminally relevant electronic (digital) information, which under certain legal procedures becomes a source of evidence in criminal proceedings. Such information, transformed into a form accessible to process participants, belongs to digital evidence. It is substantiated that investigative actions provided for by the procedural law are most often unsuitable for searching for criminally relevant information from open sources of cyberspace. It is argued that the main procedural method of forming evidence based on computer data from open sources of cyberspace should be conducting a forensic examination of electronic communications, the object of which is the initial data about the search object, cyberspace, and the subject - facts and information about this object. object In this case, methodological principles of the expert research are the intelligence tools of open OSINT

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

databases, and for recording information, the recommendations of the Berkeley Protocol, taking into account the current legislation of Ukraine. Computer data extracted from open cyberspace sources acquire probative value through the opinion of a forensic expert who is a source of evidence.

Keywords: *cyberspace; open sources of information; computer data; digital evidence; forensic science; forensic expert conclusion.*

Research Problem Formulation

Emergence of the Internet as a global network has led to a qualitatively new level of development of information services in the world and has become a technological basis for the general exchange of information. Information resources are perhaps the most important value for functioning of modern society. Unfortunately, cyberspace is also used for criminal purposes as a means of committing offenses and as a repository of criminally relevant information, including evidence. Cyberspace is an extraterritorial information territory where global processes of social communications of an international nature take place. Having emerged as a purely technical means of transmitting information, the Internet (as a component of cyberspace) has become an important social phenomenon that attracts attention of specialists in various sciences, in particular the legal one [1].

Cyberspace appearance has changed the process of proof. Information extracted from ever-evolving electronic and digital media has led to the emergence of digital evidence. Taking into account the requirements of the times, the Criminal Procedural Code of Ukraine [2] was amended in 2022: computer data was recognized as a type of document as a source of evidence (Art. 99) [3]. In procedural law, there is no definition of the terms: *computer data*, *digital evidence*, the order of their search, review, fixation, extraction and storage is not specified, which causes numerous discussions among scientists, mistakes during criminal proceedings in working with digital information, non-recognition of evidence based on it as admissible and reliable in court proceedings. Thereby, in modern conditions the question of using digital information as evidence arises. Sometimes such information is the only way to achieve the goals of criminal proceedings. Definition of procedural source of this type of evidence should be mentioned among relevant issues.

Practice demonstrates that forensically significant information has not only traces of computer crimes aimed at illegal interference with the operation of computers,

1 Гетьман А. П., Атаманова Ю. Є., Мілаш В. С. та ін. Правове регулювання відносин у мережі Інтернет : монографія / за ред. С. В. Глібка, К. В. Єфремової. Харків, 2016. С. 8. URL: https://ndipzir.org.ua/archives/5224 (date accessed: 20.05.2024).

2 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 20.05.2024).

3 Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 р. № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#n11 (date accessed: 20.05.2024).

computer programs, networks, unauthorized modification of computer data, etc., but also any computer data about illegal socially dangerous actions, which contain not only physical media, but open sources of cyberspace (websites, messengers, social networks, etc.). Well-known *Berkeley Protocol*, developed for research on open digital sources, states that information they contain is publicly available, any member of the public can view, purchase or request it without requiring special legal status or permission for unauthorized access [4].

It should be noted that information array of open sources of cyberspace is effectively used in a non-procedural form within the framework of operational-search activities as a kind of proactive operational search [5]. In foreign law enforcement practice, the so-called *Forensic Intelligence* is also used, one of the tasks of which is to search for information from open sources of the Internet [6]. At the same time (despite rapid development of information exchange processes in cyberspace), a number of legal issues remain unresolved in the domestic practice of investigating criminal offenses regarding the possibilities and features of searching and recording, the use of information from open sources of cyberspace in criminal procedural evidence.

Article Purpose

Investigate the procedural procedure for the formation of digital evidence based on information from cyberspace, access to which is not limited, in the context of evidence during criminal proceedings and substantiate the possibilities of forensic examination of cyberspace to obtain criminally relevant orienting and evidentiary information in the form of forensic expert conclusion.

Research Methods

The methodological basis of the research is modern general and special methods of scientific knowledge. Theoretical analysis and synthesis (induction, deduction, comparison, analogy, abstraction, classification) were used for research and generalization of materials from literary sources, the authors' positions on certain issues related to the subject of research; the system-structural method contributed to the consideration and isolation of the concepts of information technology in the process of proof, formal legal: disclosure of specifics and criteria for conducting investigative actions and forensic examinations. These methods are used as interrelated and complementary contributed to research completeness and the validity of

4 Berkeley Protocol on Digital Open Source Investigations / Human Rights Center, Un. Nat. Human Rights Office of the High Commissioner. New York and Geneva, 2022. P. 8. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (date accessed: 20.05.2024).

5 Волошина М. О., Шендрик В. В. Сучасні способи оперативного пошуку первинної оперативно-розшукової інформації підрозділами кримінальної поліції. *Південноукраїнський правничий часопис.* 2019. № 4. Ч. 1. С. 14. DOI: 10.32850/sulj.2019.4.1.3 (date accessed: 20.05.2024).

6 Ribaux O., Baechler S., Rossy Q. Forensic Intelligence and Traceology in Digitalized Environments: The Detection and Analysis of Crime Patterns to Inform Practice / Handbook of Security. Ed. by M. Gill. 3rd ed. 2022. Pp. 91—94. DOI: 10.1007/978-3-030-91735-7_47 (date accessed: 20.05.2024).

formulated scientific conclusions and proposals.

Analysis of Essential Researches and Publications

The problems of collecting, researching and using electronic (digital) information, computer data, and digital evidence during the pre-trial investigation of criminal offenses were studied by: H. Avdieieva, P. Antoniuk, N. Akhtyrska, S. Honhalo, A. Hutnyk, M. Hutsaliuk, V. Dyntu, A. Kovalenko, I. Kraskova, O. Krytska, T. Matiushkova, A. Novytskyi, O. Malakhova, Ya. Naidon, Yu. Orlov, D. Pashniev, O. Samoilenko, A. Skrypnyk, Ye. Skulysh, O. Starenkyi, A. Stolitnii, I. Titko, O. Torbas, V. Uvarov, Ye. Khyzhniak, D. Tsekhan, S. Cherniavskyi, V. Shkolnyi and others. In forensic publications, attention is usually focused on obtaining computer data as traces of a crime and on their transformation into digital evidence during the investigation of offenses committed most often with the use of computer technologies (cybercrimes) [7]. Traces of offenses left in the memory of computers, tablets, telephones and other devices and discovered during the inspection and search are sent for a computer-technical examination. In this case, only the amount of computer data contained in media that has entered the orbit of the investigation as material evidence or appendices to the protocols of investigative (search) or confidential investigative (search) actions is subject to search, extraction and investigation. Therefore, they are developing recommendations for the review of these computer equipment. In addition, there is a tendency among domestic scientists to adapt the old

7 Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. … канд. юрид. наук. Запоріжжя, 2008. 245 с. ; Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук. Київ, 2007. 217 с. ; Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Київ, 2020. 104 с. ; Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. … канд. юрид. наук. Харків, 2008. 191 с. ; Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. … канд. юрид. наук. Київ, 2009. 222 с. ; Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук. Київ, 2005. 218 с. ; Бутузов В. М., Гавловський В. Д., Скалозуб Л. П., Скулиш Є. Д., Тітуніна К. В., Романюк Б. В. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / за ред. Б. В. Романюка, Є. Д. Скулиша. Київ, 2011. 404 с. ; Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж : дис. … канд. юрид. наук. Київ, 2004. 217 с. ; Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за ред. А. Ф. Волобуєва. Одеса, 2020. 372 с. ; Теплицький Б. Б., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. та ін. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз : наук.-практ. посіб. Київ, 2019. 168 с. ; Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. … канд. юрид. наук. Київ, 2021. 268 с. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/02fe1a3e-438b-4f1c-8800-3e745db75e8b/content (date accessed: 20.05.2024).

recommendations on visual inspection to the new conditions of technology development. At the same time, attention is focused not on methods of extracting information, but on the procedure of recording the inspection of the relevant devices in the protocol, their sealing and transportation. Unfortunately, the procedure for identifying, recording, and extracting information from cyberspace, access to which is not limited and its use in criminal proceedings remains an understudied issue in criminology and not regulated by criminal procedural legislation.

Taking into account the criminogenic trends in the field of electronic information technologies, the constant development of technical electronic (computer) tools, software, gaps and contradictions in the legislation governing this sphere of public relations, issue of developing new and updating existing forensic methods for collecting digital evidence needs to be addressed. One of the relevant areas of research is the development of recommendations for the search for criminally relevant electronic (digital) information from open sources of cyberspace, its fixation and seizure for further use in evidence during pre-trial investigation and consideration of a criminal case in court.

Main Content Presentation

For revealing specifics of searching and using information from open sources of cyberspace during the investigation of criminal offenses, we will briefly consider the main concepts related to this process: *computer data*, *electronic (digital) information*, *media*, *traces of offenses*, *digital evidence*, *procedural means of collecting digital evidence*.

Scientists define information in the context of crimes committed using computer technologies as *virtual*, *digital*, *electronic*, *electronic-digital*, *machine*, *binary*, *computer* one, etc. The lack of a single established term is not a key problem in this field, although it certainly has significant scientific and practical significance. I order to clarify this concept, let's refer to the legislation. The laws of Ukraine and international regulations provide the following definitions:

- *"information is any information and/or data that can be stored on tangible media or displayed electronically"* [8];
- data is *"information submitted in a form suitable for its processing by electronic and means"* [9];
- *"digital content (electronic (digital) information) — any information or data in electronic (digital) form containing objects of copyright and/or related rights and can be stored and/or distributed in the form of one or more files (parts of files), records in a database on storage devices of computers, servers, etc. on the Internet"* [10];
- computer data is *"any representation of facts, information or concepts in a form that is suitable for processing in a computer system, including a program that is suitable to cause a com-*

8 Про інформацію : Закон України від 02.10.1992 р. № 2657-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (date accessed: 20.05.2024).

9 Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (date accessed: 20.05.2024).

10 Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (date accessed: 20.05.2024).

puter system to perform a particular function" [11].

The analysis of the given wording gives reason to believe that the terms *information* and *data*, *electronic (digital) information* and *computer data* are used synonymously. It should be noted that computer data or electronic (digital) information contain both meaningful (facts) and executive (performance of functions) components. In addition, the peculiarity of computer data is that the need to interpret information for human perception is inherent in their nature: they are by definition encrypted with a binary (digital) code and in their original form can only be read by computer equipment. However, this essential difference between computer data and analog data is leveled by the fact that the means on which they are stored decode information into an audiovisual form familiar to human perception (such as text, image, photo, sound, video, etc.).

Any computer data can be differentiated into two groups according to the content and meaning for the criminal proceedings process. The *first group* consists of offense-neutral information that is not relevant to criminal proceedings. Cyberspace and modern physical computer storage media contain a significant number of files of different formats and sizes at the same time, among which only a few can relate to a particular criminal offense. Therefore, the *second group* consists of criminally relevant electronic (digital) information containing:

a) data on known or wanted persons, organizations, enterprises, terrain, vehicles and other objects, events, facts, etc., that have indicative or evidentiary value in criminal proceedings;
b) traces arising at the stages of preparation, commission or concealment of the offense.

In forensic literature, there are numerous definitions of electronic (digital) traces as the results of illegal activity, the authors of which emphasize their various features. Thus, A. Kovalenko understands electronic (digital) traces of a criminal offense as computer data that were formed or changed in the memory devices of electronic computing equipment as a result of user actions related to the commission of a criminal offense [12]. The author draws attention to the forensic nature of traces as changes that occurred as a result of a criminal offense. H. Avdieieva and S. Storozhenko write that electronic digital traces are material invisible traces that can be detected, recorded and studied with the help of digital electronic devices and that contain any forensically significant information (information, data) recorded in an electronic digital form on material media. At the same time, electronic or digital devices are considered material carriers: telephones, smartphones, computers, portable geolocation devices (*GPS, Glonass*), digital cameras, video recorders, web cameras, network routers, payment systems, etc.[13]. The authors emphasize that traces of offenses are contained exclusively on electronic (digital) devices. A. Skrypnyk

11 Конвенція про кіберзлочинність : прийнята Ком. міністрів Ради Європи 08.11.2001 р. ; 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: 20.05.2024).

12 Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2022. Вип. 4 (100). С. 230. DOI: 10.33766/2524-0323.100.226-236 (date accessed: 20.05.2024).

13 Авдєєва Г. К., Стороженко С. В. Електронні сліди : поняття та види. *Там само*. 2017. Вип. 1 (77). С. 170. URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/issue/view/44/42 (date accessed: 20.05.2024).

believes that an electronic-digital trace is any forensically significant computer information, that is, information (messages, data) recorded in electronic-digital form on a physical medium or transmitted through communication channels using electromagnetic signals [14]. The last definition seems to us to be more accurate, as it implies the presence of criminally relevant information not only on the usual carriers that can be visually observed.

In our opinion, a separate carrier of criminally relevant electronic (digital) information belongs to cyberspace — an information environment in which information is in the form of symbols, images, signals and which are intended for the transfer of information in space and time. The legislator defined: "cyberspace is an environment (virtual space) that provides opportunities for communication and/or implementation of social relations, formed as a result of the functioning of compatible (connected) communication systems and the provision of electronic communications using the Internet and/or other global data transmission networks" [15]. According to the US National Security Systems Committee's glossary, cyberspace is an interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries [16].

From the forensic standpoint, cyberspace is a repository, sphere of existence of forensically significant information, which under certain legal procedures becomes the basis for sources of evidence in criminal proceedings. O. Samoilenko calls it an axiom that traces of crime in cyberspace are reflected simultaneously in many hardware of computer equipment, computer network or telecommunication network, telecommunication network [17]. According to D. Tsekhan, cyberspace means a new technical and social environment created on the basis of high information technologies and combines personal computers into an Internet network [18].

The peculiarity of cyberspace is due to the following factors: supranational and decentralized nature, the absence of a single organization that would fully coordinate and control its functioning; technological insecurity, open communication environment; the possibility of anonymous activity in computer networks, simplified user registration procedures, almost complete absence of reliable personal identifiers [19]. In characterizing the

14 Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. … д-ра філос. у галузі права. Харків, 2021. С. 74.

15 Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (date accessed: 20.05.2024).

16 Committee on National Security Systems (CNSS). Glossary. CNSSI No. 4009. April 6, 2015. P. 40. URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (date accessed: 20.05.2024).

17 Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса, 2020. С. 111. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/6d9682a6-f1ab-49a5-a609-6ca96ce3c96f/content (date accessed: 20.05.2024).

18 Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія. Одеса, 2011. С. 30.

19 Хижняк Є. С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права*. 2017. № 79. С. 160. URL: https://dspace.

essence of cyberspace, two main components can be distinguished.

The first is information and technological space containing the Internet with its resources (*Internet of Things (IoT*) and services, the *second is a* social space with users who communicate in.

Information in cyberspace exists in a qualitatively different dimension, radically different from analog. In contrast to carrier objects, which can be visually observed and whose identification features (name, type, brand, model, etc.) can be determined, cyberspace does not have such features. Instead, computer data has certain fixed characteristics, such as volume (size), format (type of information), location information (location details), time (creation, modification, use, destruction), etc. Information can be recorded with an indication of its data: website name, page, social network, time of discovery, etc. Note that a feature of computer data is their separation from the medium. That is why copying information from cyberspace leads to a change in the medium, but at the same time the data remains unchanged.

It is quite obvious: in order for computer data to be used as evidence in criminal proceedings in the future, they should be obtained in accordance with the procedural law. The need to use electronic (digital) information in proof in turn gave rise to the term *digital proof*. According to Clause 3.5 of the International Standard ISO/IEC 27037:2017, digital evidence is "information or data stored or transmitted in binary form that can be referred to as evidence" [20]. Leading Western European scientists in the field of cyber security consider electronic evidence (English: Electronic Evidence) as any information that is created, stored or transmitted in digital form, which can later be used as evidence [21]. Domestic scientists understand digital evidence as actual data that is presented in digital (discrete) form and recorded on any type of medium and that, after processing by a computer, becomes available for human perception [22]. Without going into a long scientific discussion, we note that concept lack of *digital evidence* in criminal proceedings gives rise not only to different interpretations of it by lawyers, but to an ambiguous approach to it in judicial practice [23].

onua.edu.ua/server/api/core/bitstreams/d43d895a-0cc7-4c06-9705-3b48054ecd84/content (DATE ACCESSED: 20.05.2024).

20 ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) : прийнято наказ. ДП «УкрНДНЦ» від 06.12.2017 р. № 400. [Чинний від 01.01.2019]. Київ, 2018. 31 с. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (date accessed: 20.05.2024).

21 Jones N., George E., Mérida F. I., Rasmussen U., Völzow V. Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.0. Cybercrime Division Directorate General of Human Rights and Rule of Law. Strasbourg, France. 15 Dec 2014. P. 11. URL: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf (date accessed: 20.05.2024).

22 Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. Кіберзлочинність та електронні докази / за ред. канд. юрид. наук, доц. О. Денькович, д-р права, проф. Г. Шмельцер. [Електрон. вид.] Львів, 2022. С. 133. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (date accessed: 20.05.2024).

23 Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. 2023. Вип. 1 (30). С. 126—143. DOI: 10.32353/khrife.1.2023.07 (date accessed: 20.05.2024).

Despite existing problematic situation, the legislator provided a certain list of investigative actions aimed at forming sources of evidence, the content of which is electronic (digital) information. Thus, according to the Criminal Procedural Code of Ukraine: computer data can be discovered in case of temporary access to electronic information systems, computer systems or their parts, mobile terminals of communication systems (Article 160), search (Article 236), inspection (Article 237), removal of information from power networks: communication (Article 362) or information (Article 363); during procedural actions, complete copying of information from objects of inspection, search, access is allowed; based on the results of procedural actions, sources of evidence are formed: material evidence (Article 98) or documents (Article 99); if necessary, to identify criminally relevant information, a computer-technical examination is appointed (Article 242) regarding seized material evidence or information carriers, which are appendices to the protocols of investigative and covert investigative (search) actions (Article 105) [24]. Analysis of the mentioned procedural actions shows that not all of them can be applied to search for criminally relevant information from open sources of cyberspace: for example, only information transmitted using relevant networks can be removed, and based on the results of copying information during inspection, search, temporary access, remove only those computer data contained in electronic means (Articles 160, 236, 237, 362 and 363 of Criminal Procedural Code of Ukraine) [25].

Within the framework of traditional approach, it is possible to directly discover information necessary for investigation from open sources of cyberspace in a procedural way only in the case of inspection or search during the search of enabled computer facilities. The review of computer data is carried out: a) at the scene of the incident as part of the review of computer facilities; b) as a separate investigative action during the examination of the same means seized as physical evidence; c) during the review of information copied on a specially prepared medium, which is an appendix to the protocol of the corresponding investigative action. Literary sources provide detailed recommendations on the investigative review of computer data, aimed at familiarizing with publicly available Internet resources [26], extracting information from the cloud environment [27], reviewing web pa-

24 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 20.05.2024).

25 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 20.05.2024).

26 Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія Юридичні науки.* 2023. Вип. 4. С. 55. DOI: 10.32999/ksu2307-8049/2023-4-9 (date accessed: 20.05.2024).

27 Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : кол. моногр. Львів, 2022. С. 134. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%D0%93%D1%83%D1%82%D0%BD%D0%B8%D0%BA%2C%20%D0%A5%D0%B8%D1%82%D1%80%D0%B0_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_21_06_2022.pdf (date accessed: 20.05.2024).

ges [28], searching in social networks and by IP addresses [29], etc. It is worth noting that such an inspection is admissible, since obtaining information from electronic information systems or their parts, access to which is not limited by their owner (owner, holder) or is not related to overcoming the logical protection system, does not require the permission of the investigating judge (Article 264 of Criminal Procedural Code of Ukraine) [30].

We believe that during an inspection or search, ability to search for computer data in cyberspace from open public sources of information is limited and depends on two aspects. In a simple situation, when you need to familiarize yourself, for example, with an open web page on a device that is turned on, the review is quite acceptable. In complex situations, when the source data on the search object is limited, the information that can be found in cyberspace and its volume are unknown, such a review is impractical. This is due to the following factors. *Firstly,* search for information in open sources involves the use of various special software tools and a certain research method: identification of certain information content based on primary information, analysis of newly obtained information, clarification of additional information, search again based on new data, analysis of additional information discovered, comparing it with previous information, etc. [31] This procedure can be repeated multiple times to obtain useful information. At the same time, investigative review involves conducting operations, actions and perception of the obtained results that are understandable to all participants of the investigative action. However, manipulations that, in the case of searching for information, are carried out by a specialist during the review of computer data on the basis of specific expertise using technical and software tools [32], are not obvious and are mostly inaccessible to other participants of the investigative action. *Secondly*, review (search) of data in cyberspace, taking into account the procedure described above, can take a lot of time (several hours, days or weeks) and exceed the reasonable period of investigation. In addition, in order to record the search for computer data, it is recommended to carry out continuous video recording of the device screen [33], that is appropriate only for the first of mentioned situations. *Thirdly*, if the search is carried out from an electronic device: physical evidence that is examined, then intervention in its information structure irreversibly changes initial computer data.

Performed analysis shows that established paradigm of the criminal process of dealing with computer data consists in the search, discovery and transformation of electronic (digital) information into

28 Малахова О. В. До питання огляду сторонами кримінального провадження змісту Інтернет-сторінок. *Вісник кримінального судочинства*. 2017. № 2. С. 65. URL: https://vkslaw.knu.ua/images/verstka/2_2017_Malahova.pdf (date accessed: 20.05.2024).

29 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Зазнач. твір. С. 34—37.

30 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (date accessed: 20.05.2024).

31 Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса, 2024. С. 64—81. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/content (date accessed: 20.05.2024).

32 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Зазнач. твір. С. 20—40.

33 Коваленко А. В. Організація і тактика … . URL: https://lj.journal.kspu.edu/index.php/lj/article/view/393/361 (date accessed: 20.05.2024).

analog, for which a traditional review is applied. These actions are aimed at finding and extracting computer data from media: electronic devices that can be visually perceived: personal computers, laptops, tablets, flash drives, phones, etc. The specificity of the "digital assistance" of the involved specialist in the search for information is that, due to objective reasons, he carries out most of the actions covertly, thereby actually replacing the investigator in the main, cognitive part of the investigative (search) action. Changes to the procedural law related to the introduction of computer data are mainly limited by the rules of careful description of technical means, programs for the extraction and storage of computer data as a type of document or physical evidence. However, search for information from open sources of cyberspace does not correspond to the given paradigm.

Foreign researchers point out that within the scope of digital forensics, the complete extraction and preservation of all information that could potentially become evidence is impossible: for example, for social networks due to their highly dispersed nature, huge sizes and shared ownership of data. In addition, the process of searching for data in social networks is inherently iterative (repetitive), manual search in them is impossible and therefore requires the development of special automated methods [34]. In connection with the emergence of new types of evidence, the protocol: *On the expansion of cooperation and disclosure of electronic evidence*, adopted by the Council of Europe (2022), states that not only substantive criminal law (according to new offenses), but criminal procedural law should be improved law and methods of investigation [35]. Thereby the present time requires introduction of new approaches to the process of proof using computer data contained in open sources of information in cyberspace.

Based on the above, we believe that the main procedural way to form evidence based on computer data from open sources of cyberspace should be to conduct a forensic examination. During transition to digital investigation, the objects of the expert's research should determine:

a) initial search information about the object, information about which should be found, provided by initiator of forensic examination;
b) cyberspace as a repository of criminally relevant computer data containing both evidential and indicative information about an object that is relevant to criminal offense investigation.

It would seem that this approach differs from the traditional one, according to which the expert is provided with material or materialized objects for research, which are fixed in the case materials, provided by the criminal procedural law as sources of information [36]. However, firstly, cyberspace functions on the basis of compatible (connected) communication systems that have a material origin; secondly, as stip-

34 Arshad H., Omlara E., Abiodun I., Aminu A. A Semi-Automated Forensic Investigation Model for Online Social Networks. *Computers & Security*. Oct 2020. Vol. 97. Art. 101946. P. 3. DOI: 10.1016/j.cose.2020.101946 (date accessed: 20.05.2024).

35 Convention on Cybercrime. Protocol on Xenophobia and Racism. Second Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence. Council of Europe. April 2022. Art. 1. URL: https://www.bmeia.gv.at/fileadmin/user_upload/Vertretungen/OEV_Strassburg/Dokumente/Cybercrime_-_Rechtstexte.pdf (date accessed: 20.05.2024).

36 Сімакова-Єфремян Е. Б. Комплексні судово-експертні дослідження: теорія та практика : монографія. Харків, 2016. С. 147.

ulated by the legislator, the objects of forensic examination are "phenomena and processes" [37] that take place, in particular, in cyberspace; thirdly, no objections to the expert examination of such an object will arise if the expert is provided with a medium on which, during examination, all information available at a specific moment in cyberspace regarding the subject of the investigation is copied. However, research by *International Data Corporation (IDC)* indicated that in 2020, a huge amount of data was expected to be created and used worldwide: 44 zeta bytes (44×10^{21}) [38]. It is clear that, from a technical point of view, it is impossible to have a separate removable medium that would contain the entire volume of cyberspace information.

The situation considered is similar to the purpose of the examination, when the object to be examined cannot be directly provided to forensic expert. In this case (in accordance with the Law of Ukraine: *On Judicial Examination* [39] and the Instruction on the appointment and conduct of forensic examinations and expert studies [40]), the examination initiator provides access to the object for forensic expert. In the case of cyberspace, the examination initiator, in addition to the initial data, indicates the object of research available to forensic expert without its usual direct provision.

According to existing system of forensic examinations, computer data is examined by a computer forensic science or electronic communications examination. We believe that computer forensic science cannot explore cyberspace, as the expert analyzes limited information that is physically located on the tangible object provided by the initiator to forensic expert: PCs; laptops; tablets; disks, flash drives, mobile phones and other digital information carriers [41]. The topic of computer forensic science is limited to the facts regarding the technical condition and information in electronic media [42] provided for research. In our opinion, search and discovery of evidentiary information from open sources in cyberspace should be carried out within the scope of electronic communications expertise and its new type:

37 Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (date accessed: 20.05.2024).

38 Jones N., George E., Mérida F. I., Rasmussen U., Völzow V. Op. cit. URL: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf (date accessed: 20.05.2024).

39 Про судову експертизу … . URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (date accessed: 20.05.2024).

40 Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Мін'юсту України від 08.10.1998 р. № 53/5 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (date accessed: 20.05.2024).

41 Теплицький Б. Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ.* 2021. № 3 (120). Т. 26. С. 30. DOI: 10.33270/01211203.28 (date accessed: 20.05.2024).

42 Степанюк Р. Л., Колесник В. Г. Судова комп'ютерно-технічна експертиза: стан і перспективи розвитку. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2023. Вип. 2 (102). С. 294. DOI: 10.33766/2524-0323.102.289-305 (date accessed: 20.05.2024).

informational one. V. Korshenko calls cyberspace a variety of information objects of electronic communications expertise, containing information in database formats, registration files, audio, video, text and other formats, which is on physical media and which is received, processed and transmitted using telecommunication means, systems and networks [43]. The subject of the examination of electronic communications can be defined as facts, information about the objects of search: known persons, if personal data is provided, or unknown persons, if there is only an image of the appearance, as well as about vehicles and other objects, areas of land or buildings, about organizations, connections between them and other data. It is appropriate to choose *OSINT* (*Open Source Intelligence*) open database intelligence search tools as the methodological basis of expert research, and for recording information, recommendations set forth in *Berkeley Protocol*, taking into account current legislation [44]. At the same time, a feature of expert research is not only the search for information by key features, but also monitoring, i.e., viewing specific content over a certain period of time. Obtained computer data can become the source material for the further conduct of other forensic examinations, portrait, photo-technical, linguistic, in the field of intellectual property, etc.

Conducting research on open public sources of cyberspace is especially relevant during the war in Ukraine in order to find out the circumstances of violation of the laws and customs of war, identify invaders, prove the facts of collaboration, treason, and propaganda of war [45]. An illustrative example of the possibility of obtaining important information about the object of search in cyberspace is the results of the *OSINT* section of the Information Resistance group, whose specialists found out the data of a Russian war criminal, a senior sailor, a machine gunner who fights in the Zaporizhzhia direction: his name, postal address, passport number, personal phone numbers, e-mail address, pages in social networks [46].

Conclusions

Cyberspace is a carrier of criminally relevant electronic (digital) information that is in open sources. Such information or computer data, transformed into a form accessible to the participants of criminal proceedings, belong to digital evidence. The main procedural way of forming ev-

43 Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи : автореф. дис. ... канд.. юрид. наук. Харків. 2017. 22 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/ae3bf4b6-9291-451f-bc4c-ccb5091a79e8/content (date accessed: 20.05.2024).

44 Торбас О. О. Зазнач. твір. С. 51—53, 65—99. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/content (date accessed: 20.05.2024).

45 Ragni Ch. Digital Evidence in international Criminal Proceedings and Human Rights Challenges. *Law in the Age of Modern Technologies* : International Scientific Conference on International, EU and Comparative Law Issues. Nov 2023. Art. 7:1—16. Pp. 5—6. DOI: 10.25234/eclic/28255 (date accessed: 20.05.2024).

46 Воює на Запорізькому напрямку: OSINT-секції групи «ІС» встановила дані воєнного злочинця / Інформаційний спротив. 07.05.2024. URL: https://sprotyv.info/news/voyu%d1%94-na-zaporizkomu-napryamku-osint-sekczi%d1%97-grupi-is-vstanovila-dani-vo%d1%94nnogo-zlochinczya/ (date accessed: 20.05.2024).

idence on the basis of computer data from open sources of cyberspace should be conducting a forensic examination of electronic communications. The object of forensic examination is the raw data about the search object and cyberspace, and the subject is facts and information about the search objects. Taking into account the current legislation of Ukraine, the methodological foundations of such an expert study should be the intelligence tools of open *OSINT* databases and the recommendations of the *Berkeley Protocol* for recording the obtained data. The peculiarity of electronic (digital) information extracted from open sources of cyberspace is that it acquires evidentiary value thanks to the opinion of a forensic expert, which is a source of evidence.

Відкриті джерела кіберпростору як об'єкти судово-експертного дослідження

Михайло Щербаковський

Мета роботи — за допомогою сучасних загальних і спеціальних методів наукового пізнання дослідити процесуальний порядок формування цифрових доказів за відкритою інформацією з кіберпростору в контексті доказування під час кримінального провадження й обґрунтувати можливість судово-експертного дослідження кіберпростору для отримання кримінально-релевантної орієнтувальної та доказової інформації у формі висновку експерта. Показано, що комп'ютерні дані й електронна (цифрова) інформація є синонімами та поділяються на дві групи: нейтральні, що не мають значення для кримінального провадження, і кримінально-релевантні, які містять сліди правопорушення та дані про осіб, предмети, події, факти тощо, що мають орієнтувальне або доказове значення. Доведено, що кіберпростір є окремим носієм кримінально-релевантної електронної (цифрової) інформації, яка за певних правових процедур стає джерелом доказів у кримінальному провадженні. Така інформація, перетворена на доступну для сприйняття учасниками процесу форму, належить до цифрових доказів. Обґрунтовано, що передбачені процесуальним законом слідчі дії найчастіше непридатні для пошуку кримінально-релевантної інформації з відкритих джерел кіберпростору. Аргументовано, що основним процесуальним способом формування доказів на основі комп'ютерних даних із відкритих джерел кіберпростору має стати проведення судової експертизи електронних комунікацій, об'єктом якої є вихідні дані про об'єкт пошуку, кіберпростір, а предметом — факти й відомості про цей об'єкт. Методичними засадами експертного дослідження у цьому разі є інструменти розвідки відкритих баз даних OSINT, а для фіксування інформації — рекомендації Berkeley Protocol з урахуванням чинного законодавства України. Комп'ютерні дані, вилучені з відкритих джерел кіберпростору, набувають доказового значення завдяки висновку судового експерта, який є джерелом доказів.

Ключові слова: *кіберпростір; відкриті джерела інформації; комп'ютерні дані; цифрові докази; судова експертиза; висновок експерта.*

Financing

This research did not receive any specific grant from funding institutions in the public, commercial or non-commercial sectors.

Disclaimer

Founders had no role in the study design, data collection and analysis, decision to publish, or manuscript preparation.

Participants

The author contributed solely to the intellectual discussion underlying this

document, case law research, writing and editing and assumes responsibility for its content and interpretation.

Declaration of Competing Interest

The author declares no conflict of interest related to this topic, although he is Advisory Board member of research paper collection; he was not involved in publishing decision and this article has undergone a full peer review and editing procedure.

References

Arshad, H., Omlara, E., Abiodun, I., Aminu, A. (2020). A Semi-Automated Forensic Investigation Model for Online Social Networks. *Computers & Security*. Vol. 97. Art. 101946. DOI: 10.1016/j.cose.2020.101946.

Avdieieva, H. K., Storozhenko, S. V. (2017). Elektronni slidy : poniattia ta vydy [Electronic traces : concepts and types]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka.* Vyp. 1 (77). URL: https://luhbulletin.dnuvs.ukr.education/index.php/main/issue/view/44/42 [in Ukrainian].

Avdeeva, G., Żywucka-Kozlowska, E. (2023). Problems of Using Digital Evidence in Criminal Justice of Ukraine and the USA. *Theory and Practice of Forensic Science and Criminalistics.* Issue 1 (30). Pp. 126—143. DOI: 10.32353/khrife.1.2023.06.

Berkeley Protocol on Digital Open Source Investigations (2022)/ Human Rights Center, Un. Nat. Human Rights Office of the High Commissioner. New York and Geneva. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf.

Bilousov, A. S. (2008). *Kryminalistychnyi analiz obiektiv kompiuternykh zlochyniv* [Forensic analysis of objects of computer crimes] : dys. ... kand. yuryd. nauk. Zaporizhzhia [in Ukrainian].

Borysova, L. V. (2007). *Transnatsionalni kompiuterni zlochyny yak obiekt kryminalistychnoho doslidzhennia* [Transnational computer crimes as an object of forensic research] : dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Butuzov, V. M., Havlovskyi, V. D., Skalozub, L. P., Skulysh, Ye. D., Titunina, K. V., Romaniuk, B. V. (2011). *Orhanizatsiino-pravovi ta taktychni osnovy protydii zlochynnosti u sferi vysokykh informatsiinykh tekhnolohii* [Organizational, legal and tactical foundations of combating crime in the field of high information technologies] : navch. posib. / za red. B. V. Romaniuka, Ye. D. Skulysha. Kyiv [in Ukrainian].

Committee on National Security Systems (CNSS). Glossary (2015). CNSSI No. 4009. URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

Hetman, A. P., Atamanova, Yu. Ye., Milash, V. S. ta in. (2016). *Pravove rehuliuvannia vidnosyn u merezhi Internet* [Legal regulation of relations on the Internet] : monohrafiia / za red. S. V. Hlibka, K. V. Yefremovoi. Kharkiv. URL: https://ndipzir.org.ua/archives/5224 [in Ukrainian].

Holovkin, B. M., Denkovych, O. I., Lutsyk, V. V., Tsekhan, D. M. (2022). *Kiberzlochynnist ta elektronni dokazy* [Cybercrime and Electronic Evidence] / za red. kand. yuryd. nauk, dots. O. Denkovych, d-r prava, prof. H. Shmeltser. [Elektron. vyd.] Lviv. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf [in Ukrainian].

Hutnyk, A. V., Khytra, A. Ya. (2022). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni* [Criminal procedural and forensic bases for the use of electronic documents in evidence] : kol. monohr. Lviv. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%D0%93%D1%83%D1%82%D0%BD%D0%B8%D0%BA%2C%20%D0%A5%D0%B8%D1%82%D1%80%D0%B0_%D0%BC%D0%BE%D0%BD%D

0%BE%D0%B3%D1%80%D0%B0%D-1%84%D1%96%D1%8F_21_06_2022.pdf [in Ukrainian].

Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H. ta in. (2020). Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh [Use of electronic (digital) evidence in criminal proceedings] : metod. rek. / za zah. red. O. V. Korneika. Kyiv [in Ukrainian].

Jones, N., George, E., Mérida, F. I., Rasmussen, U., Völzow, V. (2014). *Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges. Version 2.0. Cybercrime Division Directorate General of Human Rights and Rule of Law.* Strasbourg, France. URL: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf.

Khyzhniak, Ye. S. (2017). Poniattia virtualnykh slidiv ta yikh znachennia u protsesi rozsliduvannia zlochyniv [The concept of virtual traces and their importance in the process of investigating crimes]. *Aktualni problemy derzhavy i prava.* № 79. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/d43d895a-0cc7-4c06-9705-3b48054ecd84/content [in Ukrainian].

Korshenko, V. A. (2017). *Teoretychni ta metodychni osnovy sudovoi telekomunikatsiinoi ekspertyzy* [Theoretical and methodical foundations of forensic telecommunications examination] : avtoref. dys. ... kand. yuryd. nauk. Kharkiv. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/ae3bf4b6-9291-451f-bc4c-ccb5091a79e8/content [in Ukrainian].

Kovalenko, A. V. (2022). Poniattia ta sutnist elektronnykh (tsyfrovykh) slidiv kryminalnoho pravoporushennia [Concept and essence of electronic (digital) traces of a criminal offense]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka.* Vyp. 4 (100). DOI: 10.33766/2524-0323.100.226-236 [in Ukrainian].

Kovalenko, A. V. (2023). Orhanizatsiia i taktyka provedennia ohliadu kompiuternykh danykh [Organization and tactics of computer data review]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia Yurydychni nauky.* Vyp. 4. DOI: 10.32999/ksu2307-8049/2023-4-9 [in Ukrainian].

Malakhova, O. V. (2017). Do pytannia ohliadu storonamy kryminalnoho provadzhennia zmistu Internet-storinok [On the issue of reviewing the content of Internet pages by the parties to the criminal proceedings]. *Visnyk kryminalnoho sudochynstva*. № 2. URL: https://vkslaw.knu.ua/images/verstka/2_2017_Malahova.pdf [in Ukrainian].

Motliakh, O. I. (2005). *Pytannia metodyky rozsliduvannia zlochyniv u sferi informatsiinykh kompiuternykh tekhnolohii* [Issue of the methodology of the investigation of crimes in the field of information computer technologies] : dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Mykhalchuk, T. V. (2009). *Vykorystannia informatsii, otrymanoi telekomunikatsiinym shliakhom, u rozsliduvanni zlochyniv* [Use of information obtained by telecommunications in the investigation of crimes] : dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Palamarchuk, L. P. (2004). *Kryminalistychne zabezpechennia rozsliduvannia nezakonnoho vtruchannia v robotu elektronno-obchysliuvanykh mashyn (kompiuteriv), system ta kompiuternykh merezh* [Forensic support of the investigation of illegal interference in the operation of electronic computing machines (computers), systems and computer networks] : dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Ragni, Ch. (2023). Digital Evidence in international Criminal Proceedings and Human Rights Challenges. *Law in the Age of Modern Technologies : International Scientific Conference on International, EU*

and Comparative Law Issues. Art. 7:1—16. DOI: 10.25234/eclic/28255.

Ribaux, O., Baechler, S., Rossy, Q. (2022). Forensic Intelligence and Traceology in Digitalized Environments: The Detection and Analysis of Crime Patterns to Inform Practice / *Handbook of Security*. Ed. by M. Gill. 3rd ed. DOI: 10.1007/978-3-030-91735-7_47.

Samoilenko, O. A. (2020). *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori* [The basics of the methodology of investigating crimes committed in cyberspace] : monohrafiia / za zah. red. A. F. Volobuieva. Odesa. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/6d9682a6-f1ab-49a5-a609-6ca96ce3c96f/content [in Ukrainian].

Simakova-Yefremian, E. B. (2016). *Kompleksni sudovo-ekspertni doslidzhennia: teoriia ta praktyka* [Comprehensive forensic research: theory and practice] : monohrafiia. Kharkiv [in Ukrainian].

Skrypnyk, A. V. (2021). *Vykorystannia informatsii z elektronnykh nosiiv u kryminalnomu protsesualnomu dokazuvanni* [Use of information from electronic media in criminal procedural evidence] : dys. ... d-ra filos. u haluzi prava. Kharkiv [in Ukrainian].

Stepaniuk, R. L., Kolesnyk, V. H. (2023). Sudova kompiuterno-tekhnichna ekspertyza: stan i perspektyvy rozvytku [Forensic computer-technical expertise: status and prospects for development]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav im. E. O. Didorenka.* Vyp. 2 (102). DOI: 10.33766/2524-0323.102.289-305 [in Ukrainian].

Teplytskyi, B. B. (2021). *Aktualni pytannia pryznachennia ekspertyzy kompiuternoi tekhniky i prohramnykh produktiv pid chas rozsliduvannia zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system, kompiuternykh merezh i merezh elektrozviazku* [Actual issues of appointment of examination of computer equipment and software products during the investigation of crimes in the field of use of electronic computing machines (computers), systems, computer networks and telecommunications networks]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav.* № 3 (120). T. 26. DOI: 10.33270/01211203.28 [in Ukrainian].

Teplytskyi, B. B. (2021). *Tekhniko-kryminalistychne zabezpechennia rozsliduvannia zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku* [Technical and forensic support for the investigation of crimes in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks] : dys. ... kand. yuryd. nauk. Kyiv. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/02fe1a3e-438b-4f1c-8800-3e745db75e8b/content [in Ukrainian].

Teplytskyi, B. B., Sharai, L. H., Kovalov, K. M., Kuzmin, S. A. ta in. (2019). *Zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku: spetsialni pytannia kvalifikatsii, provedennia slidchykh (rozshukovykh) dii, pryznachennia kompiuterno-tekhnichnykh sudovykh ekspertyz* [Crimes in the field of use of electronic computing machines (computers), systems and computer networks and telecommunications networks: special questions of qualification, conducting investigative (search) actions, appointment of computer and technical forensic examinations] : nauk.-prakt. posib. Kyiv [in Ukrainian].

Torbas, O. O. (2024). *OSINT pry rozsliduvanni kryminalnykh pravoporushen* [OSINT in the investigation of criminal offenses] : pidruchnyk. Odesa. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/content [in Ukrainian].

Tsekhan, D. M. (2011). *Vykorystannia vysokykh informatsiinykh tekhnolohii v operatyvno-*

rozshukovii diialnosti orhaniv vnutrishnikh sprav [The use of advanced information technologies in the operational and investigative activities of internal affairs bodies] : monohrafiia. Odesa [in Ukrainian].

Voiuie na Zaporizkomu napriamku: OSINT-sektsii hrupy «IS» vstanovyla dani voiennoho zlochyntsia (2024) [Fighting in the Zaporizhzhia direction: the OSINT section of the «IS» group established the data of a war criminal] / Informatsiinyi sprotyv. URL: https://sprotyv.info/news/voyu%d1%94-na-zaporizkomu-napryamku-osint-sekczi%d1%97-grupi-is-vstanovila-dani-vo%d1%94nnogo-zlochinczya/ [in Ukrainian].

Voloshyna, M. O., Shendryk, V. V. (2019). *Suchasni sposoby operatyvnoho poshuku pervynnoi operatyvno-rozshukovoi informatsii pidrozdilamy kryminalnoi politsii* [Modern methods of operative search of primary operational investigative information by units of the criminal police]. *Pivdennoukrainskyi pravnychyi chasopys.* № 4. Ch. 1. DOI: 10.32850/sulj.2019.4.1.3 [in Ukrainian].

Zhurba, A. I. (2008). *Osoblyvosti predmeta dokazuvannia u spravakh pro kompiuterni zlochyny* [Peculiarities of the subject of evidence in cases of computer crimes] : dys. ... kand. yuryd. nauk. Kharkiv [in Ukrainian].

Shcherbakovskyi, M. (2024). Open Sources of Cyberspace as Objects of Forensic Research. *Theory and Practice of Forensic Science and Criminalistics.* Issue 2 (35). P. 10—27. DOI: 10.32353/khrife.2.2024.02.