УДК 343.982:343.148
DOI https://doi.org/10.32782/2524-0374/2022-12/105

СЛІДИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЯК ОБ'ЄКТ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

TRACES OF CRIMINAL OFFENSES AS AN OBJECT OF FORENSIC COMPUTER TECHNICAL EXPERTISE

Комісарчук Ю.А., доцент кафедри кримінального процесу та криміналістики
Львівський державний університет внутрішніх справ

Стецик Б.В., доцент кафедри кримінального права та процесу
Львівський торговельно-економічний університет

Розслідування кримінальних правопорушень, вчинених з використанням комп'ютерної техніки та комп'ютерних технологій, ускладнюється тим, що з постійним розвитком інформаційних технологій з'являються об'єкти дослідження, яких раніше просто не було, змінюються, модифікуються механізми і методи вчинення раніше відомих видів злочинів, з'являються абсолютно нові їх види. Одночасно з розвитком інформаційних технологій та інформаційних систем вченими проводяться дослідження теорії і практики протидії кіберзлочинності, розробляються алгоритмами розслідування інцидентів, аналізуються уразливості, шкідливе програмне забезпечення [1].

Проблеми якості розслідування кримінальних правопорушень і судочинства залежать від рівня розробки комплексу дієвих рекомендацій щодо їх розкриття, розслідування та попередження. Невирішеною на сьогодні залишається низка практичних проблем, пов'язаних із поводженням з електронною слідовою інформацією, призначенням та проведенням СКТЕ, використанням її результатів у кримінальному процесуальному доказуванні.

Кримінальні правопорушення вирізняються латентним характером, вони залишають обмежену кількість слідів, які є складними для виявлення, фіксації та вилучення. Зазначені обставини зумовлюють необхідність використання сучасних спеціальних знань у сфері комп'ютерних й інформаційних технологій з метою розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. У переважній більшості випадків призначення та проведення комп'ютернотехнічних судових експертиз є необхідною умовою для ефективного розслідування кримінального провадження.

Ключові слова: правопорушення, проступки, кримінальні правопорушення, об'єкт, судова комп'ютерно-технічна експертиза, доказова інформація, кіберзлочини.

The investigation of criminal offenses committed with the use of computer equipment and computer technologies is complicated by the fact that with the constant development of information technologies, objects of research appear that simply did not exist before, the mechanisms and methods of committing previously known types are complicated. changing and changing crimes, completely new types of them appear. In parallel with the development of information technologies and information systems, scientists conduct research on the theory and practice of countering cybercrime, develop incident investigation algorithms, analyze vulnerabilities and malicious software [1].

Problems of the quality of investigation of criminal offenses and judicial proceedings depend on the level of development of a complex of effective recommendations regarding their disclosure, investigation and prevention. A number of practical problems related to the handling of electronic trace information, the appointment and conduct of SCTE, and the use of its results in criminal procedural evidence remain unsolved today.

Criminal offenses are characterized by a latent nature, they leave a limited number of traces that are difficult to detect, fix and remove. The specified circumstances necessitate the use of modern special knowledge in the field of computer and information technologies for the purpose of investigating criminal offenses in the field of the use of electronic computing machines (computers), systems, computer networks and telecommunications networks. In the vast majority of cases, the appointment and conduct of computer-technical forensic examinations is a necessary condition for the effective investigation of criminal proceedings.

Key words: offenses, misdemeanors, criminal offenses, object, forensic computer and technical expertise, evidentiary information, cybercrimes.

Forensic computer and technical examination (hereinafter – SCTE) is a separate, strictly regulated procedural action, which is carried out during the investigation of criminal offenses. It is the main procedural form of using special knowledge in the field of computer technologies, and its results can represent the most important part of the evidence base in a specific criminal proceeding.

The effectiveness of the investigation of criminal offenses largely depends on the timely detection of traces of criminal acts. Criminal offenses committed with the use of computer equipment, the Internet, and cellular communications (in particular, Articles 190, 301, 333, 366-1 of the Criminal Code of Ukraine 4, etc.) cause significant material damage, while , due to the specificity of their investigation, criminals manage to remain unpunished for a long time.

Problematic aspects related to prevention, detection, use of special knowledge and investigation of crimes in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks were studied by such scientists as: V.V. Areshonkov, V.M. Atamanchuk, V.M. Butuzov, A.A. Voznyuk, V.G. Honcharenko, I.V. Hora, M. V. Gutsalyuk, A.V. Ishchenko, O.V. Kopan, O.V. Kravchuk, S.A. Kuzmin, V.I. Osadchyi, M.A. Pohoretskyi, A.A. Sakovskyi, E.D. Skulysh, O.A. Fedotov, V.G. Khakhanovskyi, D.M. Tsekhan, S.S. Chernyavskyi, Yu.M. Chornous, V.P. Shelomentsev, M.G. Scherbakivskyi, O.M. Yurchenko, and others.

During the collection of evidence in the investigation of such criminal offenses, a problem arises, caused by the fact that, along with "traditional" traces, part of the information is computer information, which does not leave changes in the external material environment, since in most cases it is informational in nature [2], and among scientists and practitioners it is interpreted differently – as electronic, digital, computer, virtual, binary information.

In the conditions of continuous penetration of information and telecommunication technologies into all spheres of public life, electronic evidence becomes the main source of evidentiary information during consideration of certain categories of cases [3]. Electronic records, e-mail, information processing files, image files are increasingly important evidence in criminal proceedings. These digital traces remain not only when cybercrimes are committed. Any of the circumstances to be proven can nowadays be presented in digital form [4]/

A characteristic feature of such information from the point of view of proof is that it can be both a direct trace of a criminal offense and a carrier of such a trace, that is, a trace object. Like any trace, computer information reflects the fact of interaction of material objects. However, such information has an excellent quality: computer information can easily be changed or destroyed, and these actions can be carried out remotely. The propriety of electronic display is determined in accordance with Art. 85 of the CPC of Ukraine. An important aspect of the propriety of an electronic display is its ability to establish a fact that is part of the subject of proof.

Studying the content of the electronic display and information in the service options of the operating system about this display, in general terms, allows you to establish: the occurrence of a crime (for example, identifying a site with prohibited content or with content that is restricted by law); the identity of the criminal (in particular, by studying his account data, establishing the IP address of the computer); the method and circumstances of the crime (for example, analyzing the content of electronic correspondence, the results of monitoring bank accounts, etc.); the nature and extent of the damage caused by the crime (which may consist of a violation of the functioning of certain electronic displays, illegal transfer of electronic funds, subscription of services (goods) not provided, forgery of documents, violation of copyright, etc.). In addition, the study of electronic display allows to confirm the facts previously established by other evidence, as well as to acquire arguments to refute the facts belonging to other investigative versions [5]. In order for these traces to turn into evidence, it is necessary to find them, to identify and record them in a procedural way. The main procedural method of turning invisible information and traces of criminal offenses into evidence is conducting a forensic examination. Therefore, the potential information found in the traces of the crime, found in electronic devices, telecommunication systems and programs, are actualized and turned into evidentiary information precisely through the use of special knowledge in the form of forensic examination. After all, the examination is an independent procedural form of obtaining new evidence and clarifying (checking) those that have already been obtained [6].

Searchable electronic information media include: diskettes, optical discs (CD, CD-R, CD-RW, DVD, DVD-RW), portable memory drives (flash), personal computer processors, memory cards personal computer cards, electronic notebooks, portable computers, mobile phones, chip cards for mobile communication services, audio and video tapes, etc. [7].

Such carriers of electronic information may contain the following evidentiary information:

a) files with text images of forged documents or graphic images of their individual fragments;

b) scanned images of the paper document and its individual details;

c) the software used to create an electronic image of the document and its details;

d) electronic assembly trace files;

e) files containing reference information on methods of forging documents;

n) stolen databases;

g) illegally copied or generated electronic digital signature codes;

f) electronic document management system software;

l) malicious programs used for unauthorized interference in the operation of electronic computing machines (computers), automated systems, computer networks or telecommunication networks;

h) software for the functioning of a printer, scanner or other peripheral equipment;

i) protocols for working on the Internet, addresses of the most frequently used websites and e-mails, e-mail messages;

s) financial and economic data ("draft" accounting), etc. [8].

The place of detection of electronic traces can be both tangible and intangible objects: Internet resources, user profile in social networks, electronic payment systems (PayPal, LiqPay, iPay.ua, "Qiwi", WebMoney, Perfect Money, etc.), databases (subscribers of communications operators, forensic records of the Ministry of Internal Affairs, etc.), local networks of various structures, "hard drives" of personal computers (laptops, tablets, etc.), memory cards, cellular communication devices and much more.

Currently, one of the technical means most often used for illegal purposes is cellular communication. They can act not only as carriers of forensically significant information, but also as objects and instruments of crimes.

For example, when extortion is committed, the actions of criminal groups are already typical, when demands are made on a mobile phone to credit the criminal's subscriber account with funds for the return of a stolen vehicle.

The following traces will be typical for criminal offenses committed with the use of cellular communication means: information traces on the carrier of the communication operator (for example, the data of the primary phone number used for communication and stored in log files; dates of the communication session communication; information about the time of communication; static or dynamic IP address logs of the provider's registration on the Internet and the corresponding phone numbers; message transfer speeds; output of logs of communication sessions, including the type of protocols used, the protocols themselves, etc.) [9]; traces on the mobile phone itself (for example, IMEI code, SMS messages, information about sent messages, telephone connections, telephone directory, telephone numbers used, traces of microparticles, fingerprints. Traces present on the SIM card and available on a mobile phone, usually identical) [10].

Therefore, electronic trace information and ways of knowing it are very closely related to the objects of SKTE [11]. After all, its generic object is a category of objects that have common features and are related to computer tools, among which software products, text and graphic documents, multimedia files, databases, application files, system reports and application logs are distinguished. Taking into account the requirements of Chapter 4 of the Criminal Procedure Code "Evidence and Evidence", it is logical to state that electronic media with media content can be classified as sources of evidence such as "physical evidence" or "documents [12]. Electronic trace information, as a carrier of information as part of material evidence, is an item containing information important for criminal proceedings, which was not created in the process of investigation (disclosure) of a criminal offense, the perception of which is impossible without the use of electronic computing devices. If we proceed from the criminal procedural regulation of work with evidence, then any content is simply computer data that has a certain consumer value and is able to satisfy the informational needs of the prosecution (or defense) during the proof of circumstances related to the subject of proof [thirteen].

Given the fact that an electronic document is a certain computer code, such a code can be read only with the help of special tools that ensure the interpretation of the digital code and its transformation into a perceptible form.

At the same time, such a feature of an electronic document as evidence determines the feature of its investigative review as a separate procedural action. An investigator or another participant in criminal proceedings cannot examine an electronic document without special means, and therefore, as a rule, such a procedural action is carried out with the help of special equipment at the investigator's workplace. At the same time, the review and study of the physical medium of the electronic document is not a study of the electronic document itself [14]. In this case, the physical medium can act only as physical evidence.

Based on the features of the review and preliminary research of electronic documents, which the investigator most often deals with in the process of investigating criminal offenses, they can be grouped into the following categories: 1) electronic documents on physical media; 2) electronic documents in the form of publications on the Internet; 3) electronic documents placed in cloud storage services [15]/

Therefore, the main property of evidence containing electronic information is verifiability. The information that makes up the content of such evidence must always be certified for the possibility of its identification and authentication, that is, checking the integrity of the information and its immutability on the electronic medium. These guarantees are mostly in the technological sphere, but ensuring the obligation of their application within the framework of criminal proceedings is the task of the criminal process. These guarantees are mostly in the technological sphere, but ensuring the obligation of their application within the framework of criminal proceedings is the task of the criminal process. The possibility of their use in criminal proceedings depends on the understanding of the nature of electronic information and its correct handling not only when conducting SCTE and other types of examinations, but also when collecting evidence containing such traces. We will focus on this in the following sections.

ЛІТЕРАТУРА

1. Шелупанов А. А. Смолина А. Р. Методика проведения подготовительной стадии исследования. Доклады ТУСУРа. 2016. Т. 19. № 1. DOI: 10.21293/1818-0442-2016-19-1-31-34.
2. Касаткин А. В. Тактика собирания и использования компьютерной информации при расследовании преступлений: автореф. дис. на соискание ученой степени канд. юрид. наук. М., 1997. С. 17–18.
3. Павлова Ю. С. Особливості збирання та процесуального закріплення електронних доказів у цивільному судочинстві. *Науковий* вісник Херсонського державного університету. 2017. Вип. 4. Т. 1. С. 77.
4. Олиндер Н. В. К вопросу о доказательствах, содержащих цифровую информацию. *Юридический вестник Самарского университета.* 2017. Т. 3. № 3. С. 108.
5. Чернявський С. С., Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства.* 2017. № 2. С. 118.
6. Коршенко В. А. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *Jumalul juridic national: teorie i practica.* 2017. №. 2. С. 192.
7. Методика расследования хищений социалистического имущества. / отв. ред. В. Г. Танасевич. М., 1980. Вып. 4. С. 162–163.
8. Осика І. М. Поняття способу підробки документів, що використовуються при вчиненні злочинів у сфері підприємництва. *Право і Безпека*. 2005. Т. 4. № 6. С. 93.
9. Потапов С. А., Потапова И. С. Использование экспертиз при расследовании и раскрытии преступлений, совершенных с применением сотовых телефонов. *Социально-экономические процессы и явления*, 2016. Т. 11. № 11. С. 157.
10. Климчук М. П. Сліди кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку, та особливості їх виявлення. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід.* К. : НАВС, 2020. С. 86.
11. Усов А. И. Концептуальные основы судебной компьютернотехнической экспертизы : дис. ... д-ра юрид. наук. М., 2002. С. 97–98. Захарко А. В., Гаркуша А. Г., Рогальська В. В., Краснобрижий І. В., Брягін О. В. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендаці. Дніпро : Дніпропетров. держ. ун.-т внутр. справ, 2019. С. 8.
12. Потапов С. А., Потапова И. С. Использование экспертиз при расследовании и раскрытии преступлений, совершенных с применением сотовых телефонов. Социально-экономические процессы и явления. 2016. Т. 11. № 11. С. 157.
13. Захарко А. В., Гаркуша А. Г., Рогальська В. В., Краснобрижий І. В., Брягін О. В. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів : методичні рекомендації: Дніпро : Дніпропетров. держ. ун.-т внутр. справ, 2019. С. 8.
14. Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Серія : Право*, 2017. № 4 (58). С. 83.
15. Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України* 2017. № 1 (88). С. 185.