


UDC 343.1:65.012.8+004


DOI: <https://doi.org/10.32631/pb.2021.4.09>

**OLEKSANDR VOLODYMYROVYCH MANZHAI,**

*Candidate of Law, Associate Professor,  
Kharkiv National University of Internal Affairs,  
Department of Cybercrime Fighting;*


 <https://orcid.org/0000-0001-5435-5921>,  
*e-mail: sofist@ukr.net;*

**ANTON OLEKSANDROVYCH POTYLCHAK,**

*Kharkiv National University of Internal Affairs;  
 <https://orcid.org/0000-0002-0973-1120>,  
*e-mail: antonpotylchak@gmail.com;**

**IRYNA ANDRIIVNA MANZHAI,**

*Kharkiv University,  
Educational department;*

 <https://orcid.org/0000-0003-2664-4472>,  
*e-mail: irinamanzhai@gmail.com*

## **ORGANIZATIONAL AND FORENSIC ASPECTS OF THE ELECTRONIC EVIDENCE HANDLING**

This paper outlines the ways of handling the electronic (digital) evidence based on the experience of the Ukrainian law enforcement bodies. It focuses mainly on the issues related to formalization and examination of the content of the electronic crime traces. Particular attention is paid to improving the arrangement of work with electronic evidence. The authors substantiate their position that the ordinary police officers need to attain the skills and knowledge how to handle the electronic evidence. The authors maintain that the nature and the mechanism of formation of electronic data are such that one may consider them as a separate kind of evidence, and the forms of registration thereof defined in applicable laws of Ukraine are far from perfect at the present time. Therefore, the article focuses on specific features pertinent to handling of the responses of institutions, enterprises, organizations; the extracted images and data from media; data banks and combinations of the aforementioned. The proposed solutions take into account the experience accrued at the time of participation in the project from interaction between the higher educational institutions and the police in the context of crime investigations.

**Key words:** *Electronic Evidence, Organizational Aspects, Forensic Aspects, Crime Fighting, Ukraine.*

### *Original article*

**INTRODUCTION.** Today, the problem of proper work with electronic traces of crimes is extremely important. It is worth noting that the problem of withdrawal and analysis of the electronic traces of the crime is interdisciplinary. That is why relevant questions are investigated in forensics, forensic examination and special investigative activity which is also called “operative and search activity” in post-Soviet countries. Moreover, it is impossible to find a solution to this problem without the involvement of technical researchers due to the nature of the electronic data itself.

Certain discussions and researches can sometimes result in fundamental rethinking of procedural steps pertinent to handling of the electronic data. For example, some forensic studies in the 1990s and 2000s in Ukraine recommended to examine next to nothing (Моїсєєв, 2001;

Стратонов, Захарченко, 2003; Шепітько та ін., 2009) or absolutely nothing (Коршенко, 2002) at the scene, disconnect computers from the network, turn the power off and send the computers to experts for examination after getting access to them within framework of the inspection, search, etc. Nowadays, the situation has changed and the movement for an old procedure of disconnecting computer equipment from the network and turning it off in most cases will result in the loss of important evidential information, which is unacceptable, and, therefore, relevant forensic procedure has been changed for the time being. Incidentally, this is specifically envisaged by DSTU ISO IEC 27037:2017 – a standard that is implemented by Ukraine in the context of identification, gathering, acquisition and saving of digital evidence<sup>1</sup>, and is also supported by the results of the

academic studies dedicated to this issue (Волков, 2018; Манжай, 2016).

The opposite effect may occur as well. For example, the expert units started to recommend avoiding seizure of keyboards, computer mice, printers and other peripheral equipment along with system blocks due to their bulkiness and mostly non-existent elements of the study. The offenders took advantage of it and went into the practice of hiding the boot modules and data storage devices in the equipment that is “exempt” from the seizure. It only took particularly thorough law enforcers to identify such counter-forensic practices and to resume comprehensive seizure procedures.

**PURPOSE AND OBJECTIVES OF THE RESEARCH.** This article serves to highlight the main organizational and forensic issues that occur during the seizure, registration and study of electronic traces of the crime and to suggest ways of addressing them.

**METHODOLOGY.** Methodological basis of this study is illustrated by quantitative and qualitative research methods. As J. J. Brent and P. B. Kraska rightly point out, by combining these methods, one will be able to enhance their strengths and mitigate their weaknesses. The study of this phenomenon gives a bigger picture of the object of the research

through the prism of different methods (Brent, Kraska, 2010). R. Tewksbury, D. Dabney and H. Copes (2010) emphasize the importance of both quantitative and qualitative methods for the conduct of legal studies.

Between 2015 and 2019, the authors and representatives of the OSCE Projects Coordinator in Ukraine conducted a questionnaire and held brief interviews with the academic and pedagogical staff of seven higher educational institutions providing special training under the auspices of the Ministry of Internal Affairs of Ukraine (19 individuals), National Police of Ukraine (94 individuals) and the Prosecutor's Office (73 individuals) from all regions of Ukraine, excluding however the Autonomous Republic of Crimea and Sevastopol. The interviewed officers of the National Police of Ukraine are holding positions in cyberpolice and counter-trafficking units. The interviewed employees of the prosecutor's office mostly serve as the prosecutor of the Office of the Region Prosecutor. Questions were related to the ways the respondents would routinely handle the electronic data during the crime investigation.

The respondents demonstrated varying albeit predictable level of computer skills (Table 1).

Table 1

Computer and Software Skills

	National Police, N/%	Prosecutor's office, N/%	Higher educational institutions of the Ministry of Internal Affairs of Ukraine, N/%
User level	48/51.1	46/63.0	3/15.8
Advanced user	41/43.6	25/34.2	12/63.2
Professional user	5/5.3	1/1.4	4/21.1
Absent	0/0.0	1/1.4	0/0.0

31,2 % of the interviewed National Police officers, 16,4 % of the interviewed prosecutor's office workers and 10,5 % of the interviewed staff of the higher education institutions of the Ministry of Internal Affairs were found to be engaged in documentation of electronic traces.

In order to identify the problems arising in the course of performance of law enforcement agencies, and to promote better understanding of the obtained results, this study involved random interviewing of the respondents in the context of documentation of the crimes that mostly have traces in electronic form. This study mainly focuses on the data gathered from the interviews pertinent to the topic of this article.

Speaking of experimental researches and observations of the performance of law enforcement agencies, D. P. Rosenbaum rightly notes that they can turn into “black boxes” unless they are supported by field observations and qualitative analysis of key processes that occur in such agencies. That is why field workers need to be heard and studied, and their activities need to be monitored (Rosenbaum, 2010).

Taking all the aforementioned into account, interim results of a pilot project that is going on in Kharkiv National University of Internal Affairs in cooperation with regional Cyberpolice units, Main Administrations of the National Police in Sumy Region and Kharkiv Region, were used at the time of writing of this article. Cadets and the academic and pedagogical staff were involved as specialists to help investigators and field officers in the study of electronic evidence within the framework of the project. Drug trafficking over the Internet,

<sup>1</sup> ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Київ, 2019. 16 с.

making and distribution of child porn over the Internet and fraud over the Internet are most frequent types of crime that this project has to deal with.

As a result, three criminal proceedings have been submitted to the court since the start of the project in February 2019. One of them concerns the activities of a criminal organization (Part 1, Article 255 “Creation of the criminal organization” of the Criminal Code of Ukraine). Moreover:

- 1) the study involved:
  - 76 electronic documents containing the information about the registration of and transactions from digital wallets;
  - 8 electronic documents containing information about the registration of and transactions involving bank payment cards;
  - 2 images of data carriers seized from the suspects;
- 2) assistance was provided in identification of 39 crime suspects;
- 3) 8 scripts and apps were developed for the use in the field service by the National Police of Ukraine.

**RESULTS AND DISCUSSION.** The substantive side of working with electronic evidence is not quite easy. For one thing, the law enforcement officers are facing the task of handling the increasingly vast amount of data comprising this category of evidence. There are times when the resources available prove to be deficient when it comes to collection and processing of data containing or capable of containing evidentiary information. This situation is typical for the majority of countries worldwide. In turn, it stimulates the law enforcement agencies to change their organizational structure and approaches to criminal investigation, becoming more technological and expand their analytical staff that can be even bigger than field officers unit. For example, according to the official data from the portal of the Federal Bureau of Investigation of the USA<sup>1</sup>, this organization has 35 000 employees. At the end of October of 2014, the majority of staff members (18 306 out of the slightly higher staff of 35 104) were engaged in support functions (intelligence analysts, linguists, scholars and information technology professionals)<sup>2</sup>. The increasing focus of the law enforcement agencies on the security func-

tions is an objective necessity, because the crime is becoming more advanced in technical and technological ways, more international and increasingly experienced in countering the efforts of the law enforcement agencies by all means possible.

The situation with electronic evidence handling particularly hard in Ukraine where territorial subdivisions are poorly equipped, in terms of hardware and software, and the technically hip personnel comes in short supply. According to the findings of the questionnaire survey, only 46 % of the interviewed police officers, 18,3 % of the prosecutor’s office employees and 31,6 % of the staff of the higher educational institutions of the Ministry of Internal Affairs were capable of telling the components of a desktop computer correctly. On the same note, 58,4 % of police officers, 50,7 % of the prosecutor’s office employees and 68,4 % of the staff of the higher educational institutions were capable of giving the accurate description of the procedure in the context of field examination of computer equipment. As one of the interviewed police officers commented,

*“The brass are usually clueless about how the computer equipment works. That is why explaining the fine details of documentation to them may prove to be quite a task. Some of them have no idea what the IP address is. They would just stare back, as if you are talking rocket science. The same goes for the external interaction... Quite honestly, skilled workers do not stay here long. They would rather go working in a private sector”.*

The latter is a typical problem for many countries, including the highly developed ones. For example, the Australian scholars D. Harkin, C. Whelan and L. Chang (2018) point out that the successful and valuable investigators from cyber units are the ones who move on to the private sector.

The absence of access to a wide range of state databases, let alone the private ones, is a problem to reckon with as well. A great number of proceedings under investigation or procedural guidance of a single person would make things worse at an arithmetic or even exponential rate. The processed and analyzed data are often not integrated into any database and, therefore, stay within the framework of one or several related criminal proceedings. This contributes to the loss of a valuable resource that could have helped in other investigations. As one of the police officers rightly noted,

*“When you come to a new place of work, it usually turns out you’re your predecessors have left nothing for you. It’s as if you have to start from scratch. And it’s the same thing with every prior job of mine. It would really help, if all processed data were collated in a single system, but who is going to*

<sup>1</sup> Mission & Priorities // Federal Bureau of Investigation : Sait. URL: <https://www.fbi.gov/about/mission> (Accessed: 06.08.2021).

<sup>2</sup> Quick Facts // WayBackMachine : Sait. URL: <https://web.archive.org/web/20141215114257/http://www.fbi.gov/about-us/quick-facts> (Accessed: 06.08.2021).

do this? And when? I have not heard about any such system existing in the police, unless some enthusiasts are doing something like that”.

Wrong internal convictions of the law enforcement officers can also be detrimental to in-

vestigation. One of the most common conviction is that software and hardware used in the study of electronic evidence need to be certified (Коваленко, 2017) (Table 2).

Table 2

**Thoughts of the Respondents about the Status of Hardware and Software Used in Handling of the Electronic Evidence**

	The number of individuals convinced that the certification is a must/total number of interviewed	%
National police	64/77	83,1
Prosecutor's office	61/70	87,1
Higher educational institutions of the Ministry of Internal Affairs of Ukraine	18/19	94,7
Total	143/166	86,14

The assumption mentioned hereinabove may come from the fact that, under the Ukrainian regulations, certification is mandatory for individual pieces of equipment wherein one intends to set up an integrated data security system, but forensic equipment is remarkably exempt from this requirement. The Register of the Forensic Examination Techniques of the Ministry of Justice of Ukraine that outlines 18 methods of hardware and software examination appears to be the only regulatory tool applicable to electronic evidence<sup>1</sup>.

Besides, one needs to mention yet another problem – no outside help can be involved, including any help within the interaction framework, because of the need to make the investigation safe. This situation can be described using the words uttered by a field officer during one of the interviews:

*“You cannot say what exactly it is all about when you are describing a problem and they are unwilling to help you because they lack motivation and understanding what kind of help you are expecting from them”.*

When it comes to development of customized software for the acquisition and the study of electronic evidence, this problem often slows the investigation down.

In the context of handling of the electronic evidence, one needs to point out the problem that the law enforcement personnel is often lacking skills and expertise required for the processing and the study of the large bodies of data. Therefore, whenever this work is carried out by regular investigators and field officers, it would be reasonable to use the simplest software solutions. This way, they will be able to perform the simple functions themselves – without the involvement of outside help (Манжай, 2019).

In our opinion, enhancement of qualification of the law enforcement officers in terms of handling of the electronic evidence is a totally feasible task. According to the studies of the means of knowledge acquisition in certain law enforcement agencies, their staff are remarkably capable of adapting to the necessity of using computer equipment in their line of work. They also appear to be practicing self-education quite actively (Table 3).

Table 3

**Ways of Acquiring the Knowledge and Skills to Operate the Computer Equipment**

	National Police, N/%	Prosecutor's, N/%	Higher educational institutions of the Ministry of Internal Affairs of Ukraine, N/%
In educational institution	29/30,9	28/38,4	9/47,4
Advanced training courses	16/17,0	17/23,3	10/52,6
Internship	47/50,0	23/31,5	9/47,4
Self-education	28/29,8	10/13,7	14/73,7

<sup>1</sup> Реєстр методик проведення судових експертиз. URL: <http://rmpse.minjust.gov.ua> (Accessed: 06.08.2021).

One of the interviewed officer of the prosecutor's office pointed out, 'In the course of our career enhancement training. We have considered specific features of working with electronic traces only theoretically. If you want to learn something, you are on your own or go ask your techie friends for help'.

Based on the findings of our studies, we believe O. Ribaux is right, saying that the modern system of police training needs to be combined. In addition to acquisition of the skills and expertise in the laws and the exclusively police work, the author also encourages the students to experiment with technologies, developing their skills in operation of the relevant software, computer models of analysis of risks and crimes, and working with huge amounts of data (Ribaux, 2019).

As regards the latter, when investigators (or their field officers) examine electronic evidence, they indeed may have to deal with certain complications because of the big amount of data that needs to be collated, processed and analyzed. A single document containing the data on bank transactions or communication details may drag the investigation out considerably, not to mention the cases when one has to deal with dozens, hundreds or thousands of such documents. A field officer point out,

*"I always feel some discomfort whenever a great number of incoming electronic documents are attached in response to my query and I need to execute an examination report on them. I usually sort them through and pick the information that is most important to the case".*

These are the most common examples of big amounts of data flooding the law enforcement agencies:

- 1) responses from institutions, enterprises, organizations;
- 2) images and data seized from devices (including the remote ones);
- 3) databases;
- 4) combinations of the abovementioned;

Let us elucidate on each point.

As regards the *responses from institutions, enterprises, organizations*, most commonly, when it comes to big amounts of data, law enforcement agencies have to deal with bank transactions, reports of providers and telecommunication operators, and responses from financial organizations. On the one hand, these documents are nothing new to the law enforcement officers. On the other hand, however, any considerable increase in the amount of data makes the examination process considerably harder and renders the old methods of analysis useless.

Following the integration of the data from such responses, one may proceed to developing

the insights which can direct the course of investigation. For example, the technique of call correlation suggested by A. Marshall and P. Miller (2019) can be used for the analysis of connection between the targets of an investigation who use cellphones with non-existent or changing IMEI, or virtual phone numbers to set a connection. This technique has already been tested in the investigation and the evidence collected in this manner has been accepted by the court.

On the early stages, law enforcement agencies try to expedite the investigation by officially requesting the information from institutions, enterprises and organizations. And this is when one may face an implicit problem of identification of the address to which any such request needs to be sent. Structurally, the organization may comprise of several subjects or it can even put in great efforts to conceal its real address. This problem is often solved by a well-established interaction with other field units, including the units from various regions of Ukraine.

The response to a request may contain information exposing the offenders. However, one may be in for some serious risks here as well. Firstly, under the Ukrainian laws, a request is not a procedural document, so the reception of the relevant information shall be formalized through the investigative process known as 'temporary access to items and documents'. Secondly, the information kept by the relevant subject may be lost, unless the investigation proceeds in a timely manner. So far, the operators are obliged by law to store the information about the connections between their subscribers but the length of such storage is not clearly defined. To avoid situations like this, big foreign providers of electronic services use specifically dedicated addresses or forms of communication with the law enforcement agencies (Вінаков та ін., 2017) through which the latter may request the storage of any information until it is withdrawn in accordance with the established procedures. Unfortunately, no such practices exist in Ukraine, so one needs to keep in touch with various institutions so as to avoid the loss of evidentiary information. The draft bill mentioned hereinabove makes provisions for introduction of the new injunctive remedies to facilitate the criminal proceedings under the title of "Temporary Data Storage". By adopting the said bill, this country will implement the well-established foreign experience in promotion of interaction between the law enforcement agencies and the private sector to the extent applicable to preservation of electronic evidence.

If the information is requested beyond the national jurisdiction, one needs to proceed with

due account for all the minute details of applicable laws in the addressee state. In this case, relevant recommendations of the expert groups from various countries<sup>1</sup> and special handbooks can be of help.

It is important to receive as complete information as possible from enterprises and organizations in an appropriate form and with the content that is relevant to the investigation. For this, one shall structure the requesting part of the relevant document in a way that will minimize the need to request any additional information in the future.

The form of the obtained information is crucial. It has to be suitable for the analysis with the use of customized software, especially spreadsheets. The inquiring party shall specifically mention it in the body of the document itself and over the phone. And information that comes in a wrong format shall be converted. Most frequently, one needs to convert documents delivered in PDF files and in the images.

Automated analysis of the obtained information can be done by the regular field officers or by the investigator who are skilled enough to operate the computer equipment on the user level. This process can be streamlined through application of:

- 1) various filters in spreadsheets with an option to select information by various criteria, e.g., full or partial information match;
- 2) means of multidimensional visual analysis of data that can help in identification of implicit connections, and in data structuring, e.g., IMB i2, Maltego, Palantir Gotham, Splunk;
- 3) applications and services for withdrawal of structural data from the files, such as:
  - identification of the bank card number and the issuing bank;
  - IP-address, making sure they belong to specific telecommunication providers (operators);
  - words and phrases, and calculation of their quantity;
  - chains of messages from an individual user for retrospective analysis of his/her activities and identification.

If the analysis automation in any specific situation is difficult or not feasible, one needs to apply the logical data processing methods.

---

<sup>1</sup> Basic Tips for Investigators and Prosecutors for Requesting Electronic/Digital Data/Evidence from Foreign Jurisdictions // United Nations : Sait. URL: [https://www.unodc.org/documents/legal-tools/Tip\\_electronic\\_evidence\\_final\\_Eng\\_logo.pdf](https://www.unodc.org/documents/legal-tools/Tip_electronic_evidence_final_Eng_logo.pdf) (Accessed: 06.08.2021).

A comparative analysis was conducted within the framework of the pilot project described hereinabove to cover the topic of the speed of execution of the examination reports in the context of documents containing large amounts of data incoming from the institutions, enterprises and organizations. The analysis was carried out using the simple methods and automated analysis systems mentioned hereinabove. According to the findings, the automated analysis expedited the execution of the examination reports by 4,2 times compared to the regular analysis methods.

When it comes to *images and data seized from data carriers*, the interests of the investigation require proper registration arrangements to be carried out within the shortest time possible and with maximum automation of this process. Secondly, the law enforcement officers have to deal with electronic data that are presented in various formats designed for a variety of operating systems. Unfortunately, according to the questionnaire findings, only 14 % of the police officers, 0 % of the prosecutor's office workers and 5,3 % of the academic-pedagogical staff have a clear understanding of the concept of an operating system. Meanwhile, 36,2 %, 66,2 % and 11,1 % of the respondents of the relevant category have no clue about the data communication protocols. With this in mind, it would be safe to assume that regular law enforcement officers require additional training to be able to carry out an independent examination of the seized images. In this particular case, acquisition of knowledge and skills in handling of forensic products that are optimum in terms of price, quality and user friendliness appears to be most topical.

Processing and analysis of the images and data seized from devices (including remote ones) most frequently proceeds with the help of:

- hardware and software packages designed for the purpose of forensic examination of mobile devices (at present, these packages are available at every single department of the National Police);
- software solutions for grabbing images of the hard disks and further examination thereof;
- traffic analysis application software.

In a conceptual article dedicated to digital forensics, E. Casey (2019) rightfully rates the forensic intelligence as one of the topmost levels of knowledge that is used for finding the solutions to the tasks of digital forensics. A combination of the forensic intelligence and the open source intelligence is the latest technique in law enforcement practices that needs to be taken into account during the handling of the seized images and data (Quick, Choo, 2018). It means that data shall be

seized from a personal computer first, and then it all shall be imported to the analytical platform in the commonly structured form. Then the additional data search on the Web shall follow. The Maltego appears to be the proper analytics platform in this case that has been successfully used by the national and foreign law enforcement agencies in crime investigations. This technique was tested within the framework of the project described hereinabove in the context of documentation of the organized crime activities and proved to be efficient.

*Databases* can be classified as a special category of structured information that needs specific processing and analysis. They can be presented in a variety of formats and, therefore, finding a common denominator for them may prove to be hard. To this end, special software can be used.

Some proceedings accumulate *all the data provided*. Processing and analysis of such data takes quite a while. It stands to reason to expect that the number of proceedings containing diverse electronic evidence will keep growing in the future. Which will exacerbate yet another problem – existing but not crucial so far – cases lining up for digital forensics in long queues. Nowadays, the waiting time for that kind of examination may take up to half a year. And no one can be sure of how long the examination itself will take. With all these problems, carrying out the investigation within reasonable timeframe may prove to be quite hard.

This is exactly why it is so important to provide career enhancement training to the field officers and investigators so that they are able to carry out simple operations with electronic evidence on their own. In addition, it is necessary to provide law enforcement agencies with the technical component that would facilitate the automation of the evidence examination process. One may engage the academic-pedagogical staff, cadets and students of specialized higher educational institutions in the process to expedite the relevant analysis. This way, on the one hand, the principle of the dual education system can be implemented for the future law enforcement officer.

On the other hand, it will be possible to facilitate the field officers and investigators in the conduct of technical forensic operations.

**CONCLUSIONS.** Introduction of innovative practices and techniques is the cornerstone of the reforming the law enforcement system. Promotion of the culture and methods of working with electronic (digital) evidence shall become one of the priorities of the relevant reforming. However, it is important to treat the object of reforming from the perspective of the complexity theory rather than as a linear system. B. Baker (2018) believes that the complexity theory suggests a way to understanding the nature and consequences of the relevant interference with the object of reforming and offers the alternative approaches to linear logical structures.

The growing tendency of introduction of computer technologies in every single area of life necessitates the rethinking of the approaches applied by the law enforcement agencies in their operation. Investigators and field officers solving numerous crimes have to deal with electronic traces which are saved one way or another, be it the data in smartphones or distributed systems. At the same time, obviously, a considerable increase in the level of the use of computer technologies by the citizens will gradually require regular investigators and detectives to collect and analyze the electronic traces on their own, for involvement of the experts in almost every criminal proceeding will be a hard task indeed. Therefore, it is vital to provide the law enforcement officers with the required technical equipment and the appropriate training.

Practitioners of the law enforcement agencies often point out that scholarly studies are often out of touch with the practical needs and reality. This problem also exists in the developed countries, so the relevant researches need to be in a language that is clear and understandable to the practitioners (Rojek, Alpert, Smith, 2012). Taking all the foregoing into account, the authors endeavored to present the findings of this article in a manner that would make them interesting and helpful to a wide range of legal professionals.

## REFERENCES

1. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій : навч. курс / А. Вінаков, В. Гузій та ін. Київ, 2017. 148 с.
2. Волков О. О. Основні джерела криміналістично значимої інформації про злочини, пов'язані зі шкідливими програмними засобами. *Innovative Solutions in Modern Science*. 2020. № 3 (22). URL: <https://naukajournal.org/index.php/ISMSD/article/download/1537/1617> (Accessed: 06.08.2021).
3. Керівництво з розслідування злочинів : наук.-практ. посіб. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. ; за ред. В. Ю. Шепітька. Харків : Одиссей, 2009. 960 с.
4. 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. 182–191.

5. Коршенко В. А. Деякі особливості поведження з комп'ютерними засобами під час проведення слідчих дій. *Вісник Харківського національного університету внутрішніх справ*. 2002. Вип. 18. С. 51–55.
6. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. Вип. 3 (74). С. 111–120.
7. Манжай О. В. Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів // Протидія кіберзагрозам та торгівлі людьми : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 26 листоп. 2019 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЕ в Україні. Харків, 2019. С. 178–180.
8. Моїсеев О. М. Залучення спеціаліста до розслідування комп'ютерних злочинів // Правові основи захисту комп'ютерної інформації від протиправних посягань : матеріали міжвуз. наук.-практ. конф. (м. Донецьк, 22 груд. 2000 р.) / МВС України, Донецьк. ін-т внутр. справ. Донецьк, 2001. С. 81–85.
9. Стратонов В. М., Захарченко С. О. Слідчі огляди у злочинах, скоєних з використанням комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2003. Вип. 24. С. 49–55.
10. Baker B. Is it complex environments or complex systems that undermines police reform in developing countries? *Police Practice and Research*. 2018. No. 19 (4). Pp. 398–410. DOI: <https://doi.org/10.1080/15614263.2018.1453982>.
11. Brent J. J., Kraska P. B. Moving Beyond our Methodological Default: A Case for Mixed Methods. *Journal of Criminal Justice Education*. 2010. No. 21 (4). Pp. 412–430. DOI: <https://doi.org/10.1080/10511253.2010.516562>.
12. Casey E. The Chequered Past and Risky Future of Digital Forensics. *Australian Journal of Forensic Sciences*. 2019. No. 51 (6). Pp. 649–664. DOI: <https://doi.org/10.1080/00450618.2018.1554090>.
13. Harkin D., Whelan C., Chang L. The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research*. 2018. No. 19 (6). Pp. 519–536. DOI: <https://doi.org/10.1080/15614263.2018.1507889>.
14. Marshall A. M., Miller P. CaseNote: Mobile phone call data obfuscation & techniques for call correlation. *Digital Investigation*. 2019. No. 29. Pp. 82–90. DOI: <https://doi.org/10.1016/j.diin.2019.03.004>.
15. Quick D., Choo K.-K. R. Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. *Future Generation Computer Systems*. 2018. No. 78. Pp. 558–567. DOI: <https://doi.org/10.1016/j.future.2016.12.032>.
16. Ribaux O. Reframing Forensic Science and Criminology for Catalyzing Innovation in Policing Practices. *Policing: A Journal of Policy and Practice*. 2019. No. 13 (1). Pp. 5–11. DOI: <https://doi.org/10.1093/police/pax057>.
17. Rojek J., Alpert G., Smith H. The utilization of research by the police. *Police Practice and Research*. 2012. No. 13 (4). Pp. 329–341. DOI: <https://doi.org/10.1080/15614263.2012.671599>.
18. Rosenbaum D. P. Police research: merging the policy and action research traditions. *Police Practice and Research*. 2010. No. 11 (2). Pp. 144–149. DOI: <https://doi.org/10.1080/15614261003593203>.
19. Tewksbury R., Dabney D. A., Copes H. The Prominence of Qualitative Research in Criminology and Criminal Justice Scholarship. *Journal of Criminal Justice Education*. 2010. No. 21 (4). Pp. 391–411. DOI: <https://doi.org/10.1080/10511253.2010.516557>.

Received the editorial office: 11.08.2021

### **МАНЖАЙ А. В., ПОТЫЛЬЧАК А. А., МАНЖАЙ И. А. ОРГАНИЗАЦИОННЫЕ И КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ РАБОТЫ С ЭЛЕКТРОННЫМИ ДОКАЗАТЕЛЬСТВАМИ**

На примере украинского опыта работы правоохранительных органов проанализированы особенности работы с электронными (цифровыми) доказательствами. Особое внимание сфокусировано на вопросах, связанных с формализацией и изучением содержания электронных следов преступления, а также на улучшении организации работы с электронными доказательствами. Обоснована позиция о необходимости приобретения навыков и знаний работы с электронными доказательствами обычными правоохранителями. Обозначено, что природа и механизм формирования электронных данных позволяют рассматривать их как отдельный вид доказательств, а определенные в действующем украинском законодательстве формы их фиксации в настоящее время не являются совершенными. Акцентируется внимание на особенностях работы с ответами учреждений, предприятий, организаций, изъятыми образцами и данными с носителей, банками данных, комбинациями перечисленного. Предложенные решения учитывают опыт, приобретенный во время участия в проекте по взаимодействию представителей высших учебных заведений и полиции по расследованию преступлений.



**Ключевые слова:** *електронні докази, організаційні аспекти, криміналістичні аспекти, протидія злочинності, Україна.*

### **МАНЖАЙ О. В., ПОТИЛЬЧАК А. О., МАНЖАЙ І. А. ОРГАНІЗАЦІЙНІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ РОБОТИ З ЕЛЕКТРОННИМИ ДОКАЗАМИ**

На прикладі українського досвіду роботи правоохоронних органів проаналізовано особливості роботи з електронними (цифровими) доказами. Увагу зосереджено на питаннях, пов'язаних із формалізацією та вивченням змісту електронних слідів злочину. За допомогою кількісних та якісних методів запропоновано шляхи вирішення проблемних питань у сфері роботи з електронними даними. Як емпіричні дані використано результати анкетування поліцейських, працівників прокуратури та науково-педагогічного складу закладів вищої освіти системи МВС України, а також проміжні результати пілотного проекту щодо протидії злочинам у кіберсфері, який реалізується в одному із закладів вищої освіти у взаємодії з регіональними підрозділами кіберполіції та регіональними управліннями поліції у двох областях України. Проміжні результати участі у проекті свідчать, що навіть проста автоматизація окремих процесів обробки й аналізу інформації в електронному вигляді здатна суттєво скоротити час розслідування.

Окрему увагу приділено покращенню організації роботи з електронними доказами. Обґрунтовано позицію про необхідність набуття навичок і знань роботи з електронними доказами пересічними правоохоронцями. Зазначено, що природа та механізм формування електронних даних дозволяють розглядати їх як окремий вид доказів, а визначені в чинному українському законодавстві форми їх фіксації сьогодні не є досконалими. На основі опрацьованих результатів показано, що правоохоронцям під час розслідування злочинів все частіше доводиться стикатися з даними великого об'єму. Акцентовано увагу на особливостях роботи з відповідями установ, підприємств, організацій, вилученими образами та даними з носіїв, банками даних, комбінаціями переліченого. Запропоновані рішення враховують досвід, набутий під час участі в проекті зі взаємодії представників закладів вищої освіти та поліції щодо розслідування злочинів.

**Ключові слова:** *електронні докази, організаційні аспекти, криміналістичні аспекти, протидія злочинності, Україна.*

**Цитування (ДСТУ 8302:2015):** Manzhai O. V., Potylchak A. O., Manzhai I. A. Organizational and forensic aspects of the electronic evidence handling. *Law and Safety*. 2021. No. 4 (83). Pp. 91–99. DOI: <https://doi.org/10.32631/pb.2021.4.09>.

**Citation (APA):** Manzhai, O. V., Potylchak, A. O., & Manzhai I. A. (2021). Organizational and forensic aspects of the electronic evidence handling. *Law and Safety*. 4(83), 91–99. <https://doi.org/10.32631/pb.2021.4.09>.