UDC 347.1

M. Shumylo, Department of Justice Taras Shevchenko National University of Kyiv Kyiv, Ukraine

R. Jurka, Mykolas Romeris University Vilnius, Lithuania

V. Kaplina, Institute for the Training of Personnel for Justice Yaroslav Mudryi National Law University Kharkiv, Ukraine

INFORMATIONAL THEORY OF EVIDENCE AND THE PROBLEMS OF USING THE ELECTRONIC MEANS OF PROVING IN CRIMINAL PROCEDURE

Abstract. *Article deals with the topical for modern science of criminal procedural law and law enforcement practice question of use in criminal procedure digital evidence. Authors highlight that development of digital technologies, electronic forms of communication, Internet, transnational and transboundary nature of crimes, which are committed in the sphere of computer information, specific nature of creation of digital tracks, gives the opportunity to state the considerable broadening of the possibilities to use in proving digital evidences, and also cause the necessity of addressing to the solving the problems of proving, which appear in the conditions of digitalization, including the heritage of informational theory of proving, which gives the possibility to adapt the probative activity in criminal procedure to any future innovative discoveries, scientific and technical progress and define the place of the digital evidence among other procedural sources of evidence. During the research, it is found the factors, which influence negatively on the law enforcement practice, lead to recognition the evidence obtained in criminal proceeding as inadmissible. It is emphasized, that the cognitive potential in the aspect of development of the science of criminal procedure has the informational theory of criminal procedural proves. Relying on the fact that digital technologies are based on the methods of coding and transporting information using double code of encryption, which gives the possibility not only transport the information, but also recognize it after that, authors make the con-*

clusion about suitability to use wider concept of «digital information» and «digital evidence» instead of concepts «electronic information» or «computer information». In order to formulate relevant conclusions, the authors refer to the legislation of foreign countries. The results of the study are formulated in the conclusions, where authors suggest definition of the concept of digital evidence and state the need to distinguish the digital evidence as an independent processual source of evidence.

Key words: *evidence in criminal procedure; digital information; electronic information; electronic document; informational technologies.*

Introduction

The development of digital technologies, electronic communications, the Internet has caused significant impact on social life and legal rules. Computers, mobile phones, artificial intelligence, the use of electronic money and cryptology have become commonplace for many of us. In the conditions of digital reality, the law as a whole and the criminal procedural law in particular gradually change. However, despite the updating of the criminal procedural law, it still does not meet the needs of the present. During proven activity in criminal proceedings, the latest technologies of fixing traces of a crime, and the identification of persons who committed it are increasingly being used, but not always received information is used as evidence in court or may be grounded in a court decision. Factors that negatively affect law enforcement practices, in our opinion, are of a systemic nature and are, first of all, due to the lack of proper legislative tools; and secondly, to the theory of proof that meets the needs of time, contains the concept of evidence and proving, according to which the procedural status of "digital information" becomes clear. In addition, legal terminology, which is contained in the law or which is used in the legal doctrine, has dialectical unity with the process of law enforcement. Meanwhile, it should be noted that there is no unity in the approaches to understanding such concepts as "computer evidence", "digital evidence", "digital information", "electronic document", "computer information", "electronic media" "a document made using computer technology", etc. All above mentioned obviously requires addressing the problem of evidence in a digitalisation environment, which will allow the adaptation of proving activity in criminal proceedings to any future innovation achievements and determination of the place of digital (electronic) evidences among procedural sources of evidence.

Problems of legal regulation of use of digital (electronic) information as evidence in various aspects were investigated in the works of O. S. Aleksandrov, V. D. Arseniev, M. S. Alekseyev, V. S. Balakshin, A. R. Belkin, J. P. Borulenkov, V. B. Vekhova, B. Ya. Gavrilova, V. P. Gmyrka, L. V. Golovko, V. Ya. Dorokhov, N. A. Zygury, Z. Z. Zinatullin, S. V. Zuev, A. Yu. Kalamayko, I. O. Krytska, O. S. Kuchin, V. O. Lazareva, P. A. Lupinskaya, O. P. Metelev,

I. D. Naidis, P. S. Pastukhov, C. B. Rosinsky, M. S. Strogovich, D. M. Tsekhan, S. A. Sheifer, A. V. Shilah and others. The growing scientific interest in the abovementioned problems should be noted as a positive point. At the same time, the scholars mainly concern only certain aspects, the doctrine of criminal procedural law is not studied comprehensively, in particular, at the dissertation level, in which the problems of the legal nature of electronic means of proving, their classification, epistemological and methodological basis of use in proving would be solved; proposals regarding effective legal regulation of the use of digital information would be formulated; the legal regulation of the use of digital technologies in the course of proving in the criminal process of foreign states would be analysed, etc.

Consequently, the purpose of the article is to develop scientifically grounded approaches to solving problems arising when using electronic means of proving in a criminal proceeding; their consideration through the prism of the information theory of evidence; definition of the ratio between the concepts of ""digital" and "electronic" evidence", "digital" and "electronic" information; development of features of digital evidence; definition of its concept; establishment of the place of digital evidence in the system of procedural sources of evidence; study of foreign experience of legal regulation of use digital evidence in proving.

1. Materials and methods

In order to achieve the purpose of the article and to formulate substantiated conclusions, in the process of work a complex of general scientific and special methods of scientific research, which are traditional for legal science was used: dialectical, formal and logical, hermeneutical, generalisation and comparative and legal. The dialectical method, absorbing the entire system of categorical apparatus of dialectics and operating during the cognition with the principles of reflection, activity, comprehensiveness, ascension from the individual to the general, and on thecontrary from the general to the one, the interconnection of quantitative and qualitative characteristics, determinism, the unity of induction and deduction, analysis and synthesis, made it possible to study the problems arising from the use of digital evidence in criminal proceedings from the point of view of the integrity of this legal phenomenon and the interconnectedness of its element. Ascension thinking from specific to abstract, with the subsequent transition from abstract to specific, allowed establishing essential, typical and generalised features, characteristic for understanding the legal nature of digital evidence, to emphasise their individual and specific features. The formal and logic method became the basis to disclose and improve the notion of digital evidence, to compare it with other concepts used in legislation and doctrine. With the help of the hermeneutic method, the legal content of certain norms of the criminal procedural and civil procedural legislation was established, the fact that legal terminology does not correspond to the modern achievements of the technical sciences was revealed. Using

the comparative legal method, the authors learned the legislative tendencies of foreign states. The method of generalisation made it possible to consistently integrate single facts into a single whole and formulate substantiated conclusions aimed at improving the normative regulation of the issues under investigation, and overcoming the problems that are encountered in enforcement practice. These methods were used in the interconnection, which contributed to the completeness of the research and the validity of the formulated scientific conclusions and proposals.

2. Results and discussion

2.1 Information theory of evidence as promising vector of scientific researches in terms of digitisation of the proving process

In the theory of procedural law of the end of 19th – early 20th the notion of "evidence" was defined as everything that filled the world with matter, all that may be perceived by us from the spiritual world [1]; or as totality of grounds to believe that there are circumstances, which must be established in the present case [2]. Such an understanding of the notion of "evidence" was due to the time, corresponded to the development of the science of procedural criminal law, and therefore significantly differed from that existing in the domestic doctrine of the criminal process and legislation.

In the Soviet period, there was view of evidence as facts learned by a court during the administration of justice. Such a vector of understanding of evidence was developed by such scholars as A. Ya. Vyshinsky, M. O. Cheltsov, S. V. Poznyshev [3–5]. However, such an understanding of evidence was not devoid of deficiencies. Emphasising that the above definition of evidences leaves the question of the origin of the fact unclear, it as if appears before a subject of proving to be in the finished form, M. S. Strogovich proposed the "double" concept of the notion of evidence, the essence of which was that the notion of evidence unites: 1) a fact on the basis of which necessary circumstances of crime are established and 2) the source provided by law from which a subject of proving obtains the facts [6]. M. S. Strogovich understood sources of facts as types of evidence common to modern science of the criminal process: testimony, expert opinions, material evidence, protocols, reviews, other written documents, etc.

In the 60s of the last century, in conditions of rapid development of technological progress, the issue on informational nature of evidence became topical. V. Ya. Dorokhov was the first who mentioned this aspect of evidence; he can be considered the founder of the information theory of evidence. According to this theory, evidence is reviewed not as a fact, but as information about the fact that it is an information signal [7]. The information theory of V. Ya. Dorokhov is based on the theory of reflection, the main thesis of which is the postulate that the outside world objectively exists and can in principle be known. The author concluded that evidence is result of interaction of two

material objects, each of which leaves own mark on others. Therefore, the mechanism of evidence formation is in system of "double reflection". First of all, objects of the surrounding world interact with each other, leaving trace-reflection on one another or in the consciousness of witnesses of interaction – this is the "primary reflection". Later, the traces left are revealed by a subject of evidence and are already reflected in his/her mind during the review of the place of the event, interrogating eyewitnesses, which is a "secondary reflection". Information, in the opinion of V. Ya. Dorokhov, being in its essence a reflection of past events, is of signal nature and cannot exist separately from matter: its existence is always conditioned by presence of information source and its receiver. The same evidence is the unity of information (information) and their source (material carrier) [8].

Consequently, within informational theory, evidence is information (data or message) that is transmitted through signal and is an encoded equivalent of an event, recorded by a carrier of information and expressed in the form of conditional physical symbols, which creates a certain ordered set [9]. Such understanding of evidence can be perceived by modern science, which has faced the necessity of the transformation of approaches to understanding evidences in criminal proceeding, that in its turn is conditioned by significant changes in economy and society as a result of digitalisation and the forthcoming fourth industrial revolution [10].

2.2 The essence and features of electronic evidence, its place in the system of procedural sources of evidences

The Law of Ukraine of October 3, 2017, "On Amendments to the Commercial Procedural Code of Ukraine, the Civil Procedural Code of Ukraine, the Code of Administrative Justice of Ukraine and other legislative acts" introduced such a means of proof as an electronic evidence in the procedural codes [11]. The legislator uses unified approach to understanding of "electronic evidence" as information in electronic (digital) form that contains data about circumstances important for a case, in particular, electronic documents (including text documents, graphic images, plans, photographs, video and audio, etc.), websites (pages), text, multimedia and voice messages, metadata, databases, and other data in electronic form. The law provides that such data may be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, back-up systems, and other places of data storage in electronic form (including the Internet).

At the same time, the legislator has neglected the need for such changes in the criminal procedural law, which has already been discussed among legal scholars and practitioners. On January 17, 2019, Verkhovna Rada of Ukraine adopted draft law № 9484 "On Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (regarding the improvement of the order of application of certain measures for the enforcement of criminal proceedings)." Despite the fact that the developers announce in the explanatory

memorandum that the draft law provides for amendments to the CPC of Ukraine in terms of clarifying the special terminology in the field of information technologies, the text does not define the notion of electronic (digital) evidence or at least electronic (digital) information [12].

In our opinion, the absence of appropriate changes to the criminal procedural legislation can only be explained by the conservatism of the domestic legislator. Thus, law-enforcement practice is forced to adapt the current CPC to the needs of the present, and "electronic evidence" in criminal proceeding are considered material evidences or documents that not always corresponds to the nature of the latter (art. 98, 99 of the CPC) [13]. Such "adaptation" does not always find support in the courts, and the evidence obtained is deemed inadmissible. Thus, it is obvious that there is a need to improve the legal definition of the notion of evidence in criminal proceedings, taking into account the specifics of digital information, as well as the normative consolidation of the special regime for its use and verification. It also confirms the thesis that it is necessary to allocate electronic (digital) evidences as a separate procedural source of evidence and the inability to identify them with material evidences and documents.

It is known that terminology has the important place in doctrine and lawmaking. Each legal term has a legal sense and with the help of a legal notion reflects an essence of a legal phenomenon or process. Therefore, it is no coincidence that terminology used in legislation and science is the subject of close attention and discussion. This is about equation or, on the contrary, separation of the concepts of "digital" and "electronic" evidence. Thus, M. O. Efremova defines "electronic information" as information (messages, data), presented in electronic and digital form, regardless of the means of their storage, processing and transmission [14]. A similar position is taken by V. M. Shchepetylnikov, who believes that the totality of social relations connected with the circulation of information cannot be exhausted by the use of the term "computer", since the computer is only one of the varieties of electronic computing technology. In this regard, the author prefers the use of the term "electronic information" [15].

The opposite position is taken by the American scientist Joseph Rotenberg, who argues that the notion of "digital information" is more appropriate because information theoretically can exist in non-electronic form, for example, with the use of optical and quantum technologies, and "electronic information" is not necessarily digital [16]. S. P. Kushnirenko also emphasises the expediency of using the term "digital information". According to his understanding, digital information is any information presented in the form of a sequence of digits available for input, processing, storage, transmission through technical devices [17].

Ukrainian legislator equates the notions of "digital" and "electronic" information and, consequently, there are

"digital" and "electronic" evidence, in particular, in the norms of the Civil Code of Ukraine. Basing on the legislator's approach domestic scientists also equate these notions, using the terms "electronic" and "digital" evidence as synonyms [18].

In our opinion, such the position is more convincing according to which it is appropriate to use the broader notion of "digital information" and "digital evidence", since digital technologies are based on methods of encoding and transmitting information using a dual encryption code (0 and 1), which allows not only the transmission of information, but also it recognition after receipt. Electronic information (and computer information) is only a kind of digital information and correlates with the latter, respectively, as kind and class.

Taking into account requirements of time, modern scientists try to develop the definition of the notion of electronic evidence. In particular, A. I. Zozulin understands digital information as information that is encoded in a dual system of computation and is transmitted using any physical signals [19].

Also it is proposed to understand as digital evidence any information (messages, data) that is in electronic form on the basis of which a court, prosecutor, investigator basing on a certain established procedural order, determines the presence or absence of circumstances to be proven during the criminal proceedings, as well as other circumstances relevant to a criminal case [20].

On the basis of the formulated definition, the authors propose a number of features of electronic evidence, among which are the following: 1) they are represented in encoded form in one of the objective forms of information existence – electronic; 2) they are always mediated through technical material carrier beyond which their existence is impossible; 3) simultaneously several participants of the criminal proceedings may have access to them and acquaint with them; 4)evidence is quickly transformed into non-electronic forms and vice versa; for example, they can be printed on paper and scanned from a paper carrier; 5) there is a possibility to copy them on any type of electronic media and to send on any distance; 6) evidence is collected, investigated and used for the purpose of criminal proceedings only with the help of special scientific and technical means – means of storage, processing and transmission of computer information, information and telecommunication networks and terminal equipment [20].

In general, it is worth agreeing with the proposed features of digital evidence and emphisisng that, in our view, key one is the absence of material form because they cannot be felt due to the lack of material expression. Meanwhile, digital evidence can exist in intangible form on technical media. These features distinguish electronic evidence from written and material evidence. In addition, it should be added that digital information is more vulnerable to third-party intervention, it can be easily destroyed or changed. The process of creating and storing information is also specific; it makes it easy to change a carrier without losing content and, on the contrary, pro-

vides the ability to make changes to the content without leaving traces on a carrier. In addition, the transmission and copying of digital information is possible without removing a carrier using which this information was created.

2.3 Features of using digital information in foreign countries

To create updated domestic model of proving, which corresponds to modern level of achievements of science and technology, from the perspective of search the ways to solve similar problems, it is important to analyse foreign practices in order to learn from advanced countries. In addition, the transnational and transboundary nature of crimes in the field of computer information, the use of computers as tools for committing a crime, the specific nature of the creation of digital traces outside the jurisdiction of one particular state entails the development of intergovernmental cooperation and, possibly, the formation of a unified international application law information technology in criminal proceedings.

The use of digital evidence in the United States, which is considered a pioneer in computerisation, is governed by the Federal Criminal Procedure Code [21], the Federal Rules of Evidence [22], Manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations [23], the Federal Law "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (so called "the USA Patriot Act") [24], the Foreign Intelligence Surveillance Act [25], as well as judicial precedents. In the United States there are also a number of rules, instructions, and techniques aimed at regulating the use of electronic evidence.

Unlike in the Ukrainian legislation, in the United States there is no legal definition of evidence. The norms of the federal rules of evidence also do not contain any mention of digital or electronic evidence, which is explained by the fact that this act was adopted in 1975, but the evaluative concepts and their functional interpretation allow the distribution of the provisions of the Rules to the current needs, as evidenced by the textbooks, practical comments and scientific articles. Also, the absence of exhaustive list of evidence in the procedural legislation of the USA gives such an opportunity [22].

In the doctrine, evidences are defined as information that is able to establish or refute a fact [26]. Article 401 of the Federal Rules of Evidence establishes a rather evaluative notion that evidence is appropriate if it can, in any form, make any fact which has an effect on the qualifications of an offence to be more likely or less probable than in the absence of this evidence [27]. In this, evidences are divided into three categories: 1) real or physical evidence that consists of tangible objects that can be seen and touched; 2) testimony of witnesses, which may be provided in court proceedings on the basis of personal observation or experience; 3) indirect evidence, based on additional information, observation of reality, which can

confirm the conclusion, but does not prove it (so they are considered as indirect).

Definition of digital (electronic) evidences is also developed in the theory of American criminal proceeding. Digital (electronic) evidence is any evidentiary information stored and transmitted in digital form, which a party to a lawsuit may use in a court session [28]. The legislation does not provide list of procedural actions that are used to collect digital evidences.

Usage of digital evidence in the process of proving in the USA is regulated in details in Manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Chapter V). In the Manual, electronic documents as evidences are divided into non-hearsay and hearsay [23].

By the origin and content there are two main groups of computer evidences: 1) evidences as a result of activity of a person stored on an electronic carrier and containing information filled in by a user; 2) evidences created by a computer in accordance with in accordance with the program laid down (*computer-stored evidence, human generated computer evidence*);

Non-hearsay evidence includes those that generated by a computer without a human participation; such evidences are divided onto two categories: *computer-generated records* (records created by a computer) and *computer-stored records* (records that are stored in a computer) [29].

The result of human activity (personal letters, memos, accounting documents, etc.) are reviewed as *hearsay.*

In this, the Manual establishes a list of requirements for an electronic document as procedural evidence. Before accepting an electronic document as evidence, a process participant must prove its authenticity, which allows to establish the admissibility and conclude that the authenticity is correct. This approach is due to the fact that evidences created by a human is more vulnerable to interference and changes than the evidence that is created directly by a computer. Consequently, the main thing in the American proof theory is the possibility of verifying the evidence that conditions its admissibility.

In France, according to Part 1 of Art. 427 of the CPC of France, the presence of crimes can be established using any type of evidences that allow a judge to make a decision based on his/her own conviction. Consequently, the CPC of France does not contain an exhaustive list of types of evidence. In addition, the CPC of France consolidates the freedom to collect evidences, any act of an investigating judge which he/she considers necessary to do, except in cases explicitly prohibited by law, may be admissible [30].

In the CPC of Germany, although direct digital information is not isolated as an independent source of evidence, based on the CPC, it can be concluded that such information can be collected during any procedural action: seizures, mailboxes, telephone conversations, searches, examination of documents, telecommunications control, computer search, possible criminals, etc. [31].

Conclusions

The development of digital technologies, electronic forms of communication, the Internet, the transnational and transboundary nature of crimes committed in the field of computer information, the use of computers as tools for committing a crime, the specific nature of the formation of digital traces, including beyond the jurisdiction of a particular state, make it possible to ascertain the significant expansion of the possibilities to use digital evidences in proving, as well as condition the necessity to address the problems of proving that arise in the conditions of digitalisation, including relying on the acquisition of the information theory of evidence, which will allow to adapt evidence in criminal proceedings to any future innovation achievements, scientific and technological progress and determine the place of digital evidence among procedural sources of evidence.

Factors that adversely affect law enforcement practice lead to the recognition of evidence obtained in criminal proceedings as inadmissible, they are of systemic nature and related to the lack of proper legislative tools. The theory of evidence, which meets the needs of the time, contains the concept of evidence and proving, according to which the procedural status of "digital evidence" becomes clear, as well as the lack of unified terminology and awareness of its legal content.

The scientific potential in the aspect of the development of criminal procedural science is the information theory of criminal procedural evidences, which, based on the information theory, explains the essence of judicial evidence as information signals coming from the objective reality in a mind of a subject of evidence and contributes to the formation of the corresponding cognitive images.

The essence of electronic evidence must be investigated through their peculiarities, inherent features that reflect the specifics and legal nature of electronic evidence, and using which they can be distinguished as an independent form of evidence.

Relying on the fact that digital technologies are based on the methods of encoding and transmitting information using dual encryption code, which allow not only transmitting of information but also recognizing it, there is the logical conclusion it is more expedient to use more wide term "digital information" and "digital evidence". Electronic information (and computer information) is only a kind of digital information and correlates with the latter, respectively, as kind and class.

It is necessary to understand as digital evidence any information (messages, data) that is in electronic form on the basis of which a court, prosecutor, investigator basing on a certain established procedural order, determines the presence or absence of circumstances and facts relevant to a criminal proceeding, an investigation of which can be conducted using special program and technical means.

References

1. Vladimirov, L. V. (2000). *The doctrine of criminal evidence.* Tula: Avtograf.
2. Smirnov, A. V. (2000). *Models of the criminal process.* St. Petersburg: Nauka, LLC Publishing House "Alfa".
3. Vyshinsky, A. Ya. (1950). *Theory of forensic evidence in Soviet law.* Moscow: Legal Publishing House of the National Committee of the USSR.
4. Cheltsov, M. A. (1948). *Criminal proceedings.* Moscow.
5. Poznyshev, S. V. (1923). *Proofs in criminal proceedings.* Moscow – Leningrad: Jurid. Publishing house NKYU USSR.
6. Strogovich, M. S. (1968). *The course of the Soviet criminal process: the main provisions of the science of the criminal process.* Moscow: Nauka.
7. Rossinsky, S. B. (2014). On the prospects for the development of the information theory of criminal procedural evidence (in connection with the possibility of departing from the postulate of Marxist-Leninist philosophy). *Bulletin of the Samara State University,* 11–2 (122), 73.
8. Dorokhov, V. A. (2016). The concept of evidence. In N. V. Zhogin (Ed.). *Theory of evidence in the Soviet criminal process.* Moscow: Nauka.
9. Gritsanova, A. V. (Ed.). (2003). *Newest Philosophical Dictionary.* Minsk: Interpresservice LLC.
10. Klaus, S., & Davis, N. (2018). *Technologies of the fourth industrial revolution.* Moscow: Eksmo.
11. On Amendments to the Commercial Procedural Code of Ukraine, the Civil Procedural Code of Ukraine, the Code of Administrative Legal Proceedings of Ukraine and other legislative acts: Law of Ukraine dated October 3, 177, No. 2147-VIII. Retrieved from http://zakon.rada.gov.ua/laws/show/2147–19.
12. On amendments to the Criminal Procedural Code of Ukraine and the Criminal Code of Ukraine (regarding the improvement of the procedure for the application of certain measures for the enforcement of criminal proceedings): Draft Law of Ukraine dated January 17, 1948, No. 9,984. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65354.
13. Criminal Procedural Code: Law of Ukraine dated April 13, 2012 No 2227-VIII. Retrieved from https://zakon.rada.gov.ua/laws/show/4651–17.
14. Efremova, M. A. (2012). On the concept of computer information. *Russian Justice,* 7, 50–52.
15. Shchepetylnikov, V. N. (2006). *Criminal law protection of electronic information* (Candidate thesis, Yelets State University named after I.A. Bunina, Ryazan, Russian Federation).
16. Rothenberg, J. (1999). *Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation.* Amsterdam: European Commission on Preservation and Access.
17. Kushnirenko, S.P. *Digital information as an independent object of forensic investigation.* Retrieved from http://www.law.edu.ru/doc/document.asp?docID=1311821.
18. Kalamayko, A. Yu. (2017). *Electronic proof in the civil process.* Kharkiv: Pravo.
19. Zozulin, A. I. (2018). *Legal and methodological basis of digital information in evidence in criminal cases* (Candidate thesis, Ural State Law University, Ekaterinburg, Russian Federation).
20. Zuev, S. V. (Ed.). (2018). *The development of information technology in criminal proceedings.* Moscow: Yurlitinform.

21. Federal Rules of Criminal Procedure. Retrieved from https://www.law.cornell.edu/rules/frcrmp.
22. Federal Rules of Evidence. Retrieved from https://www.law.cornell.edu/rules/fre.
23. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. (2009). Retrieved from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.
24. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. Retrieved from https://www.justice.gov/archive/ll/highlights.htm.
25. The Foreign Intelligence Surveillance Act of 1978. Retrieved from https://it.ojp.gov/privacyliberty/authorities/statutes/1286.
26. Shcherbakov, S. V. (2010). *American criminal evidence law: English-Russian reference dictionary.* Moscow: Yurlitinform.
27. Best, A. (2017). *Evidence.* New York: Wolters Kluwer.
28. Brenner, S. W. (2011). *Digital Evidence and Computer Crime: forensic science, computer and the internet.* Amsterdam: Elsevier.
29. Kerr, O. S. *Computer Records and Federal Rules of Evidence. United States Depart-ment of Justice.* Retrieved from http://euro.ecom.cmu.edu/program/law/08–732/Evidence/KerrComputerRecords.pdf.
30. Code de procédure pénale. Retrieved from https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154.
31. The German Code of Criminal Procedure. Retrieved from https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

Published: Вісник Національної академії правових наук України. 2019. Т. 26. № 2. С. 137–152.