

DOI 10.5817/MUJLT2019-1-5

WEB-PAGE SCREENSHOTS AS AN EVIDENCE IN CIVIL PROCEDURE OF UKRAINE*

by

NELLI GOLUBEVA**, KRISTINA DROGOZIUK***

Currently the question about the possibility of including a screenshot of a web-page to the base of evidence in civil procedure of Ukraine remains open. The problem is a lack of systematic rules for determining procedures for obtaining electronic evidence, in particular, screenshots, in Ukrainian legislation, as well as possibilities for their use while considering civil cases. Various electronic evidence should correspond various admissibility criterias, and therefore the admissibility of electronic evidence should be examined separately according to each type of evidence.

Separate issues of investigation, fixation and certification of web-screenshots as evidence in civil procedure of Ukraine are considered in this article. The analysis of legal regulation and problems of the practical implementation of use of web-pages screenshots in Ukrainian civil procedure are carried out. The ways of implementation of recommendation rules for registration and fixation of web-screenshots in civil procedure, which can be applied for all European states, are proposed.

KEY WORDS

Civil Procedure, Civil Procedure of Ukraine, Electronic Documents, Electronic Evidence, Means of Proof, Proving, Screenshots, Website

* The authors would like to express their gratitude to the reviewers, MUJLT Editor-in-Chief *Jakub Harašta* and editor *Lenka Pastušková*, who immensely helped to improve the quality of the manuscript.

** *nelli@email.ua*, Professor, Head of the Department of Civil Procedure, Faculty of Civil and Commercial Justice, National University "Odesa law academy", Ukraine.

*** *kristina.drogoziuk@gmail.com*, Senior Lecturer, Faculty of Civil and Commercial Justice, National University "Odesa law academy", Ukraine.

1. INTRODUCTION

In time of information technology an important problem in protection of rights and interests is provision of collection, fixation and certification of evidence obtained from the Internet.

Electronic devices which are used every day for solving domestic, life, professional and other issues, due to their prevalence among users and functionalities, may also contain evidence, and sometimes this means of proof may be the only evidence in case, or have more probative value in comparison with other evidence during consideration and resolving of a particular civil case.¹

The relevance of the chosen topic is due to increase in digital information and its systematic use in various spheres of life, which determines the need for further scientific research and a clearer legislative regulation of use of electronic evidence in civil procedure, as well as introduction of optimal approaches to information technologies in proving in civil procedure of Ukraine.

The judicial practice of recent years has shown that there are categories of civil cases in which the dispute has arisen over information posted on the Internet. In this category of cases, courts are forced to add to the case some files and investigate information received from the Internet.

Focusing on this topic is related to the fact that recently Ukrainian law has significantly developed in the question of electronic evidence, while currently there are many European states that either do not have such rules for electronic evidence.

The purpose of this research is to suggest some improvements to the mechanism of investigation, fixation and certification of web-screenshots in civil litigation, which can be useful both in Ukraine and in European countries.

2. ELECTRONIC EVIDENCE IN UKRAINE

It should be mentioned that the Internet is a way of placing and disseminating information that may involve a wide variety of civil cases which are connected with the illegal use or distribution of intellectual

¹ Laz'ko, O. (2015) Prospects for the development of electronic (technical) means of proof in the civil process of Ukraine. *Evropeyski perspektivy*, 1, pp. 125–129.

property objects; with protection of honor, dignity, business reputation; with breach of consumer rights protection, etc.

It should be emphasized that in theory of civil procedural law of Ukraine, the main criteria for the admissibility of “computer evidence” were determined in 1999. In particular, the following criteria were formulated: a document that was issued by a computer when it was used continuously for the accumulation and processing of information in any type of activity that was carried out at the same time; during this period the information was sent to the computer in the usual order; the whole period of work with the document computer functioned properly; the information in the document reflected the information that came to the computer in the usual way.² One of the main criteria for electronic evidence is the ability to identify the source by which this evidence was obtained.

Until adoption of the Law of Ukraine No 2147-VIII of October 3, 2017, which was significantly amended Civil Procedure Code of Ukraine (hereinafter referred to as *CPC of Ukraine*), no one normative legal act provided a special procedure for investigation and use of evidence placed on the Internet. In current CPC of Ukraine Part 7 of Art. 85 was included, according to which the court, on the application of the participant of the case or on its own initiative, may inspect the website, other places of data storage on the Internet in order to establish and fix its content.³ Consequently, under the current CPC of Ukraine, a court has judicial authority to investigate the global network directly for the presence of certain facts that are in the subject of evidence in the case.

However, despite of such positive developments, CPC of Ukraine still does not sufficiently regulate issues regarding procedure for submission and certification of originals and copies of electronic evidence, order and peculiarities of the investigation and evaluation of such evidence by the court. Obviously, the lack of the normative regulations of the highlighted issues may lead to ambiguous judicial practice and make difficulties in use of electronic evidence in civil procedure.

² Reshetnikova, I. and Yarkov, V. (1999) *Grazhdanskoe pravo I grazhdanskiy process v sovremennoy Rossii* [Civil law and civil process in modern Russia]. Moscow: Izdatelstvo Norma, p. 178.

³ Pavlova, Iu. (2017) Some aspects of the admissibility of electronic evidence in the civil procedural procedure law of Ukraine. *Prykarpatskyi yurydychnyi visnyk*, 5 (20), pp. 83–87.

As *Petrenko* emphasizes, that problems of legal regulation and the use of electronic evidence are parts of a wider problem of introduction of electronic and information technologies in litigation as a whole. In the legislation of many countries there were rules governing the use of electronic technologies in the consideration and resolution of cases by the court. Some countries already have a great deal of practical experience in using and standardizing electronic technologies at the trial.⁴ For example:

- in Germany – Informations-und Kommunikationsdienste-Gesetz of June 13, 1997;
- in Australia – An Act to facilitate electronic transactions, and for other purposes, 1999;
- in the USA – Electronic Signatures in the Global and National Commerce Act, which came into force on October 1, 2000;
- in the UK – Electronic Communications Act 2000;
- in Canada – The Personal Information Protection and Electronic Documents Act of 2000 and the Canada Business Corporations Act, the Canada Cooperatives Act of 2001.

Paying attention to ways of ensuring the admissibility of electronic evidence, it is possible to note that in 1983 in the US a court has determined that in order to recognize the electronic evidence as admissible, it should be based on scientific knowledge and facilitate the understanding or verification of the facts by a judge or jury.⁵

3. WEB-SCREENSHOTS AND ISSUES OF ITS' USE IN CIVIL PROCEDURE OF UKRAINE

Web-screenshot is a picture of the selected area of the screen of the device that displays the relevant web-page at the time of fixation of this image.

Web-page screenshots as evidence in litigation can be used for fixation:

- the fact of placing information on the Internet that does not correspond to reality or violates exclusive rights;

⁴ Petrenko, V. (2018) Electronic evidence as an element of information technology in civil justice. *Molodyi vchenyi*, 1 (53), pp. 111–115.

⁵ *Daubert v. Merrell Dow Pharmaceuticals Inc.*, U.S. Supreme Court. *United States Reports*, vol. 509, pp. 579–601, 1983.

- the confirmation of the fact of information on the Internet that infringes copyrights;
- the confirmation of improper performance or non-fulfilment of contractual obligations by other party in a case;
- another legally relevant information posted on the Internet.

However, there are many issues while using this type of evidence.

Firstly, any page on the Internet may be changed or, in general, deleted; also access to it may be blocked. There is a question of technical review of the page and access to information about its state in a retrospective, at the particular moment in the past.

Secondly, there is a complexity of identifying the person who disseminated negative information on the network or proving his (her) involvement in such dissemination. Given the specifics of the existence and operation of the Internet, any person may carry out various insulting messages and remain unknown at this time, which creates the procedural impossibility of filing a lawsuit for the plaintiff in light of norms of Art. 175 of CPC of Ukraine. Other important problems are *fixation of commission of an offense* and *fixation of a date of commission of an offense*.

Thirdly, *the absence of an official sample of a screenshot*, which would indicate the compliance with the document form, or the systematic rules of execution a screenshot and lodging it with the court, significantly complicates its use as evidence in a case.

Fourthly, sometimes non-recognition of a screenshot as evidence is due to *the inability to reproduce it in the original*.

The rapid development of computer technology and appearance of a variety of new programs facilitates counterfeiting, distortion or even destruction of information in electronic form, which will make it impossible or significantly difficult to investigate and evaluate electronic evidence by court. Consequently, a court may take into account false evidence and establish the circumstances of the case in a wrong way. This problem is only partially regulated by Art. 423 of CPC of Ukraine by consolidating such basis for reviewing of case with newly discovered circumstances as the falsehood of electronic evidence. However, CPC of Ukraine does not contain a mechanism for protecting electronic evidence from distortion or destruction.

4. WEB-SCREENSHOTS OBTAINED FROM SOCIAL NETWORKS

A particular attention should be paid to the issue of the admissibility of web-screenshots obtained through social networks. Considering the ability of social networks to bring information about a large number of people, it is particularly essential to use data from social networks during consideration of cases about honor, dignity and business reputation protection, or about false information.⁶

Social network accounts in fact are reflections of a person's personality, and therefore in everyday life actions in social networks are considered to be committed on behalf of that person. Meanwhile, the abovementioned statement does not find its normative substantiation, which makes it difficult to recognize web-screenshots from social networks permissible. For example, in social networks like *Facebook*, *Instagram*, *Twitter*, anyone can register with any name and distribute false information. The connection between person and false information in social networks is hard to prove.

That is, the problem of the permissibility of screenshots obtained from social networks is to ensure the identification process of the person who created or distributed certain information in the social network.

Usually, defendants in cases where it is necessary to use electronic evidence from social networks, make the permissibility of such evidence doubtful, referring to the fact that no identification processes are carried out during the registration of the social network accounts, and therefore any person could register under the name of the defendant and do anything.

The use of false accounts was the subject of investigation by the *High Specialized Court of Ukraine for Civil and Criminal Cases* in a judgment of 22. 2. 2017 in the civil case *No 761/13156/16-ts*, during which the court of cassation noted that providing a legal assessment of the printed screenshot of a person's Facebook page, the *Court of Appeal* proceeded from impossibility to identify holders of accounts, located on resources/links in Facebook and the possibility of creating a fake account on this network. However, the *Court of Appeal* did not pay attention that some of the information on the defendant's Facebook page contained placemarks,

⁶ Pavlova, Iu. (2017), op. cit.

confirmation of his location at a certain time at a particular place and a personal nature of certain information, rather than publicly available.⁷

In this case, the court examined not only content of a particular record, in which the information, according to the plaintiff, contained inaccurate information, but also the account as a whole on the availability of personal information, indicating the inextricable interconnection between the identity of the defendant and the relevant account in social network.⁸

Although the position of the cassation court raises certain procedural concerns, it is worth recognizing that this position is rather progressive, forms separate criteria for the permissibility of electronic evidence obtained from social networks, and in future may serve as a case law for lower courts.

5. FEATURES OF USING OF AN ELECTRONIC DIGITAL SIGNATURE IN WEB-SCREENSHOT

While Ukraine has accumulated a rather low experience in legal regulation of electronic document management and e-commerce, in the UN system and in the European Union these relations have already gained a significant development. The Association Agreement between the EU and Ukraine provides the harmonization of national legislation with EU law, therefore, it is worth to pay attention on the following legislative acts.

Two Model Laws: on Electronic Commerce (MLEC, 1996)⁹ and Electronic Signatures (MLES, 2001)¹⁰ have been created by the *United Nations Commission on International Trade Law – UNCITRAL*. These laws promoted legal status of electronic documents.

Art. 6 and 7 of the UNCITRAL Model Law on Electronic Commerce states that if the law requires written information, that requirement is met by a data message, if the information contained therein is accessible so as to be usable for subsequent reference.

⁷ Decision of the High Specialized Court of Ukraine for the consideration of civil and criminal cases from 22. 2. 2017, Case No 761/13156/16-ц. [online] Available from: <http://www.reyestr.court.gov.ua/Review/65038960> [Accessed 17 January 2019].

⁸ Pavlova, Iu. (2017) Some aspects of the admissibility of electronic evidence in the civil procedural procedure law of Ukraine. *Prykarpatskyi yurydychnyi visnyk*, 5 (20), pp. 83–87.

⁹ UNCITRAL Model Law on Electronic Commerce (1996). [online] Available from: https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf [Accessed 17 January 2019].

¹⁰ UNCITRAL Model Law on Electronic Signatures (2001). [online] Available from: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf> [Accessed 17 January 2019].

Where law requires a signature of a person, that requirement is met in relation to a data message if:

- 1) the method is used to identify that person and to indicate that person's approval of the information contained in the data message;
- 2) the method is as reliable as was appropriate for the purpose data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

However, this statement is sufficiently general because it does not establish criteria for the method's compliance with the listed requirements. The answer, and further guarantees of the legal validity of information in electronic form (validity of the proposal, acceptance, and electronic evidence) can not be included.

In view of this, UNCITRAL Model Law on Electronic Signatures, which clarified a number of important issues, was further created. It specified more detailed requirements for electronic signature.

Firstly, it was stated that an electronic signature should be directly related to the person who signed the document. This means that the signature should exclude ambiguity with regard to the person.

Secondly, signing, at the moment when it is carried out, must be controlled only by the signatory. It is assumed that the person, expressing his (her) will, signs the document, and no one can put his (her) signature without his (her) knowledge. If anyone acts on behalf of another person(s), the general rules of representation are applied.

Thirdly, any change in the electronic signature made after signing must be available for identification. This requirement, firstly, does not affect the changes to the signed document, and secondly, does not mean that the changed signature is no longer valid. The fact is that all changes must be known to the counterparty, which will make a decision. This requirement, that signatures are made using cryptography tools is standard for EDS, but not necessary for other types of electronic signature. Therefore, drafters of the law have introduced a restrictive condition for the application of this requirement.

Two directives have also been adopted in the European Union: The Electronic Signatures Directive 1999/93/EC (no longer in force)¹¹ and The Electronic Commerce Directive 2000/31/EC¹².

On 1 July 2016 The Electronic Signatures Directive 1999/93/EC was repealed by eIDAS (electronic IDentification, Authentication and trust Services). It was established in the Regulation (EU) No 910/2014 of 23 July 2014¹³. The regulation has applied directly to EU Member States and establishes a common standard for electronic signatures, electronic stamps, time stamps, eDelivery services and website authentication certificates in the internal market.

All organizations delivering public digital services in EU member state must recognize electronic identification from all EU member states from 29 September 2018.

It would seem that the regulation is an internal matter of the EU, but in reality, it is also used by foreign contractors who deal with European organizations. Although each country has its own identification and electronic digital signature (EDS) standards, eIDAS is a set of “best practices” that guarantees EDS compatibility at the European level, because all public organizations of the EU are obliged to recognize qualified EDS from other countries. In future, it is likely that eIDAS will expand its operation beyond the EU.

The Electronic Commerce Directive establishes a general requirement for the recognition of documents signed by electronic signature: EU member states should ensure that restrictions related to the use of electronic signatures should not significantly impede contractual relations between parties and deprive documents signed by an electronic signature of equal legal force in relation to traditional documents.

¹¹ Directive 1999/93/EC of European Parliament and of Council of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive). *Official Journal of European Communities*. L 13. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093> [Accessed 17 January 2019].

¹² Directive 2000/31/EC of European Parliament and of Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in Internal Market (Directive on electronic commerce). *Official Journal of European Communities*. L 178. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031> [Accessed 17 January 2019].

¹³ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of European Communities*. [online] Available from: <https://eur-lex.europa.eu/eli/reg/2014/910/oj> [Accessed 6 May 2019].

Currently, the use of electronic signatures in Ukraine is regulated by Laws of Ukraine: *On Electronic Trust Services*, *On Electronic Documents and Electronic Document Transfers*, *On E-Commerce*, and others.

The Law of Ukraine *On Electronic Trust Services* includes such concepts as “electronic signature”, “advanced electronic signature” and “qualified electronic signature”.

To become an owner of electronic digital signature it is necessary to apply to an accredited centre of key certification (ACKC). There are several dozen centres in Ukraine today. The activity of ACKC is carried out on the basis of the relevant license and certificate. The activity of the ACKC, as a commercial entity, is controlled by the *Central Certification Body* (Ministry of Justice of Ukraine) – a state organization that regulates relations in the field of electronic signature.

It should be noted that according to Part 2 of Art. 100 of CPC of Ukraine, Art. 1 of the Law of Ukraine *On Electronic Trust Services* and Part 1 of Art. 5 of the Law of Ukraine *On electronic documents and electronic document circulation*, electronic evidence or its copy without electronic digital signature, equivalent to a personal signature, cannot be considered as a reliable evidence. This means that the signing of electronic evidence by EDS is mandatory in the Ukrainian legislation.

It can be concluded that electronic evidence must be created using a specific system, access to which is obtained through a special electronic key issued by the authorized body.

In electronic correspondence, correspondence in messengers or social networks login and password to the system can be seen as simple electronic signature (as the system is holding the logs of the steps which were made under the login – thus e.g. in e-commerce platforms, we can talk about signing the electronic document when, for example, goods are ordered by clicking on the virtual buttons).

Evidence, if the document (log) belongs to some person, are thus incorporated in the metadata, which are held by the system provider. The reason for that is that simple electronic signature is very broadly described in Art. 3/10 eIDAS Regulation as

“data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign”.

Article 1/12 of the Law of Ukraine *On Electronic Trust Services* reproduces the specified norm and states that electronic signature is the electronic data, which is added by the signer to other electronic data or logically connected with them and used by him (her) as a signature.

In practice it becomes clear that until e-mail services, social networks, messengers do not require a copy of passport to register a new page, there is no evidence of belonging of them to a specific person and unscrupulous participants of litigation can use fake names. Thus, a judge has to decide on the relevance of such evidence.

6. WEB-SCREENSHOT – AN ORIGINAL OR A COPY OF ELECTRONIC EVIDENCE?

According to possibility of unobstructed copying of electronic evidence without limiting the number of copies and without any loss of their qualitative characteristics in the process of copying, it is possible to predict appearance of certain practical problems for the participants of the case, regarding the separation of the original electronic evidence from its copy, as well as the certification of electronic copies and paper copies of electronic evidence.¹⁴

Thus, there is still a question what can be considered as the original of electronic evidence. As a result, the court may have questions about the permissibility and legal assessment of the evidence. For example, will be considered as the original a video or a screenshot, filed on a CD or on a flash memory card or other media, if it was made with the help of a webcam, then saved on the Internet and then copied to a CD or a flash memory card? Similar questions may arise regarding videos, sound recordings, or screenshots made during a live stream on the *Youtube* service and, accordingly, saved on the server of this service. *Petrenko* emphasizes that the subsequent copying of such a video or photo on a CD will not be considered as an original.¹⁵

Part 3 of Art. 100 of CPC of Ukraine establishes that parties of the case have the right to submit electronic evidence in paper copies certified in accordance with the procedure prescribed by law. That is, civil procedural law defines web-screenshot as a copy of electronic evidence.

¹⁴ Petrenko, V. (2018) Electronic evidence as an element of information technology in civil justice. *Molodyi vchenyi*, 1 (53), p. 113.

¹⁵ Ibid.

At the same time, participant, who submits a copy of electronic evidence, must indicate who has an original electronic evidence. If original electronic evidence is not filed and party of the case or court has some doubts on the conformity of submitted copy of an original, such evidence is not taken into account at the trial. However, as noted above, information that is posted on the Internet can be easily changed or even deleted.

To solve this problem, an amendment was added to CPC of Ukraine, which is on the possibility of carrying out an inspection of electronic evidence at their location in case of impossibility of its delivery.

7. CARRYING OUT AN INSPECTION OF ELECTRONIC EVIDENCE AT ITS LOCATION

In accordance with Part 7 and 8 of Art. 85 of CPC of Ukraine, the court on the application of a participant of the litigation or on its own initiative, may inspect the website, other places of data storage on the Internet in order to establish and record their contents.

The applying of evidence inspection at its location is possible on condition that the electronic evidence has not been removed from the place of data storage. It happens quite often, when in a case a court does not have access to the original of electronic evidence. Due to the lack of a clear definition of the concept of “original electronic evidence” there may be doubts about its permissibility in the case when it has been copied to a CD or other information carrier, since in this case evidence can be considered as an electronic copy, not the original.¹⁶

To resolve these contradictions, it seems advisable to amend CPC of Ukraine with Article 100-1 in which to define the concept of “original electronic evidence” and “copy of electronic evidence” as follows:

The original electronic evidence is information in electronic form that has a set of mandatory requisites and/or properties that makes such information unique and different from other similar electronic evidence. Graphic (digital) images, videos and recordings saved on various electronic information carriers are used as originals of electronic evidence and can not be considered as electronic copies, except when the source of such objects is the Internet (created directly on the Internet).

¹⁶ Ibid.

Copy of electronic evidence is created by electronic (digital) means or reproduced on paper, and corresponds to the original and certified in accordance with the procedure established by the law.

It is worth emphasizing that the difference of information on the website of the provided copy of the screenshot is not an obstacle to use it as evidence, since in this case it is already a question of either faking the screenshot or changing the website, which should be established by appropriate expertise.

8. COMPUTER-TECHNICAL EXPERTISE FOR SETTING AND FIXING THE CONTENT OF THE WEBSITE

It should be underlined that today we can talk about the problem of the low level of training judges for work with software and hardware complexes and complex software shells. It is impossible to obtain equivalent knowledge after reading books or having communication with a specialist. In this regard, the involvement of a specialist while working with electronic evidence is mandatory, since the least unskilled action can lead to the loss of important evidence or guidance information.¹⁷

The court has a right to appoint a computer and technical expertise to establish and record the content of the website, other places of data storage on the Internet, on condition – if it requires special knowledge and can not be carried out by the court independently or with the specialist's participation.

According to Art. 1 of the Law of Ukraine *On Forensic Examination*, forensic examination is a research on the basis of special knowledge in the field of science, technology, art, crafts, etc. concerning objects, phenomena and processes in order to provide an opinion on questions that are or will be the subject of judicial review. According to the results of computer-technical expertise, the expert will be able to determine the actual location of the server, which provides the activity of the offender, as well as to investigate the contents of the server itself, even to recover deleted files, determining the date of their creation and placement.¹⁸

There is no doubt that electronic evidence obtained through the Internet, examined in the order prescribed by Art. 85 of CPC of Ukraine, will fully

¹⁷ Tsehan, D. (2013) Digital evidence: the concept, features and place in evidence system. *Naukovyi visnyk Mizhnarodnogo humanitarnogo universytety. Iurisprudencia*, 5, pp. 256–260.

¹⁸ Ibid.

comply with the requirements for the permissibility of electronic evidence, and therefore can be used in civil disputes resolution.

Expert examinations are carried out by certified court experts in relevant specialties, which are included in the register of court experts of the Ministry of Justice of Ukraine.¹⁹

During an expert research on the object of intellectual property that is contained on the website occurs:

- domain name verification, installation of DNS servers;
- checking the IP address matching;
- fixing the display of the content of the site, the display of the main page, transitions to pages of interest to the applicant;
- determining the time of creating a web page;
- research data are recorded in the research part of the conclusion, the survey results (web-pages, photographs, screenshots, etc.) are made by the inspection report with the indication date.

9. NOTARY CERTIFICATION OF WEB-SCREENSHOTS

In order to use electronic information as evidence in Ukrainian civil procedure there were some attempts to substantiate the position regarding the possibility of providing screenshots to the court, certified by a notary as evidence. However, this practice is not widespread and in most cases plaintiffs provide simple printouts of information from the website to the court.²⁰

In CPC of Ukraine all cases of notarial certification of copies of documents are allocated separately. Art. 95 of CPC of Ukraine states that the party has a right to provide a copy of written evidence, certified by his (hers) own signature. However, Art. 100 of CPC of Ukraine states that a written copy of electronic evidence is not a written evidence. From this it turns out that Art. 95 of CPC of Ukraine does not regulate the issue of how a paper copy of electronic evidence should be certified.

Consequently, the question arises in which way a paper copy of electronic evidence is required to be certified, what is generating a gap

¹⁹ Okhromeev, Yu. (2012) Collection of evidence base in cases of violation of rights in the Internet. [online] Available from: http://uba.ua/documents/text/27_01_2012_Okhromeev.pdf [Accessed 17 January 2019].

²⁰ Lezhuh, T. (2013) The use of electronic evidence in cases relating to the protection of honor, dignity and business reputation. *Viche*, 16, pp. 13–15.

in the law. Because of this, judges do not know how to comply with such an ambiguous rule of law and could apply it incorrectly; besides, they will not take responsibility, because formally the violation of the process will not take place because of a gap in the procedural law. Sometimes, because of this gap in the law, electronic evidence is unlawfully unconnected, and, conversely, some evidence is added contrary to the law. In such cases, the rights of participants in the process concerning the accession of evidence and the basis of legal proceedings are violated, and with it parties' rights to a fair trial.²¹

Therefore, it is no accident, that the question of the possibility or impossibility of fixation by the notary of information obtained from the Internet is considered sufficiently debatable among lawyers. Since some scholars think that a notary can provide evidence from the Internet,²² while others put forward technical and legal objections.²³

The scholar *Kucher* states that the necessary confirmation of the execution of a transaction is the introduction of the relevant information in the register, their perception by the notary or reproduction through the use of computer technology products.²⁴ Indeed, for the purpose of committing important notarial actions by the notaries today, it is necessary to check the absence of prohibitions of alienation of real estate objects, the existence of state registration of ownership of a specific owner, etc., which are contained directly on the Internet, but such important information may be distorted or specifically presented in a distorted form on computer of a specific notary.

Considering this issue from the standpoint of the notarial process, we can set a threat to ensure not only the notarial secrecy, but also the reliability of the information that notaries receive through the Internet for the commission of notarial actions. *Badila* emphasizes that for the investigation of this type of evidence it should be provided a legal and

²¹ Draft Law on Amendments to Article 100 of the Civil Procedural Code of Ukraine (regarding the certification of copies of electronic evidence). [online] Available from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63876 [Accessed 17 January 2019].

²² Yacenko, O. (2013) Providing evidence by notaries, or neighboring experience, which is lacking in Ukrainian lawyers. *Yurydychnyi zhurnal*, 5 (131), pp. 60–67.

²³ Afyan, A. (2013) The role of the notary in the process of proving the facts regarding information in the Internet. *Civilisticheskaya processualnaya musul'*. *Mezhdunarodnyi zbornik nauchnykh statey*, 2, pp. 119–125.

²⁴ Kucher, T. (2013) Features of the application of evidence created with the help of computer technologies in the notarial process. *Civilisticheskaya processualnaya musul'*. *Mezhdunarodnyi zbornik nauchnykh statey*, 2, p. 153.

technical expertise to answer questions regarding the possibility of notaries to secure evidence, which are available on the Internet.²⁵

Art. 75 of the Law of Ukraine *On Notary* determine that notaries, officials of local self-government bodies who carry out notarial actions, certify the fidelity of copies of documents issued by enterprises, institutions and organizations, provided that these documents do not contradict the law, have a legal value and certification of their loyalty copies which are not prohibited by the law.

However, now Ukrainian notaries refuse to implement the protocol for reviewing the web-page due to the lack of such a notarial action in the Law of Ukraine *On Notary* and in the Order of notarial actions by notaries of Ukraine.

Consequently, a situation arises when a person can provide a court with a printout from a website where false or insulting information has been disseminated, and then, after receiving a statement of claim, the person who distributed it can easily remove it, making impossible to prove its existence. On the one hand, in such a situation, the plaintiff can apply for confirmation the existence of information to a person providing hosting services (placing a website on the Internet) or to the Internet service provider. And on the other hand, such information may not always be collected by such person. In addition, it often takes a lot of time to receive it (for example, assignment of orders to the courts of other states).

Sometimes, plaintiffs try to claim through a court reference from providers in the form of log-files (with a list of actions of users and placement of data), since obtaining such a reference in pre-trial order is virtually impossible. According to the Law of Ukraine *On Telecommunications*, operators and providers of telecommunications are obliged to provide and carry responsibility for the security of information about the telecommunication services provided, including the receipt of services, their duration, content, routes, etc.

Consequently, Ukrainian law emphasizes that personal information may be disseminated either in the presence of a written consent of the consumer, or at the request of the inquiry authority, investigator, prosecutor or court within the bounds of a criminal or operative-investigative affair.

²⁵ Badila, O. (2014) Evidence and the need to provide them with a notary and a court: topical issues. *Nashe pravo*, 4, pp. 156–161.

Recently, a draft law No 8281 dated April 17, 2018 *On Amendments to Article 100 of CPC of Ukraine (regarding the certification of copies of electronic evidence)* was registered in Verkhovna Rada of Ukraine, which is an unconditional positive step towards the settlement of the use of screenshots in civil procedural law.

Adoption of the bill will provide an opportunity to deal more quickly with cases in which electronic evidence is present. Judges will not have to question the correctness of the application of certain rules of law. The implementation of the bill will remove doubts as to the compliance of the original of attached materials with cases and copies of electronic evidence. As a result of adoption of the bill, the procedural rights of citizens will be ensured.²⁶

A notary, as a person authorized by law, will be in position to assume responsibility for the fact that paper copy has been taken from a certain electronic evidence. In addition, the notary has the technical ability and access to all necessary registries for such certification. At the same time, the notary will take the responsibility for the false information of the certified data.

It also seems advisable to regulate the rules and requirements for drawing up a screenshot in civil procedure law of Ukraine. One of the forms of fixing information on the Internet in the world is the notarial certificate of the content of the electronic page.

In connection with the lack of procedures for the provision of electronic evidence by notaries in Ukrainian legislation, if there is a reason to think that filing evidence will subsequently become impossible or complicated, Ukrainian lawyers will have to turn to the notaries of the Russian Federation, whose legislation provides such a notarial action.

Articles 102–103 of the Fundamentals of Legislation on the Notary of the Russian Federation provide the implementation of notaries' activities to provide evidence.²⁷ As a part of its activity to provide evidence, notary often conducts a review of the website or content of the e-mail. Notary inspect a site and describes its content in detail. The result is a protocol

²⁶ Draft Law on Amendments to Article 100 of the Civil Procedural Code of Ukraine (regarding the certification of copies of electronic evidence). [online] Available from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63876 [Accessed 17 January 2019].

²⁷ Fundamentals of the legislation of the Russian Federation on notary, Federal Law of 11. 2. 1993, No 4462-1. [online] In Russian. Available from: https://www.consultant.ru/document/cons_doc_LAW_1581 [Accessed 17 January 2019].

of reviewing a website, which is fixed by a notary's seal. Also Article 103.9 regulates the certification of the equivalence of the document on a paper medium and an electronic document. It consists in confirming the identity of the content of the submitted electronic document to the notary in the contents of a paper notarized document.

A document made on a paper carrier made by a notary has the same legal validity as an electronic document, the equivalence of which is certified by a notary. The electronic document submitted to the notary must be signed by a qualified electronic signature.

Tripulsky stresses that this norm can also be used in Ukraine in accordance with Art. 12 of the Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters (October 7, 2002), which is valid both for Ukraine and for Russian Federation.²⁸ Thus, documents, which are issued or certified by the competent authority or by the specifically authorized person within its competence and in the prescribed form and affixed by the stamp in the territory of one of the Contracting Parties, are accepted on the territories of the other Contracting Parties without any special certificate. Documents which are considered as official documents in the territory of one of the Contracting Parties use evidence power of official documents in the territories of other Contracting Parties.²⁹

Website review by the notary of Russian Federation consists of the following steps:

- verification of the domain name, installation of DNS-servers;
- verification of IP-address;
- checking the accuracy of displaying the content of the website with a browser to which it refers;
- displaying referrals to pages, which are interesting for the applicant.

²⁸ Minsk Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters (7. 10. 2002). [online] Available from: <http://cisarbitration.com/wp-content/uploads/2017/02/Minsk-Convention-on-Legal-Assistance-and-Legal-Relations-in-Civil-Family-and-Criminal-Matters-english.pdf> [Accessed 17 January 2019].

²⁹ Tripulskiy, G. (2015) Some aspects of the admissibility of evidence obtained on the Internet in the civil process. *Tsyvil'ne sudochnystvo u svitli sudovoi reformy v Ukraini: materialy mizhn. nauk.-pract. konf. im. Yu. S. Chervonogo* [Civil Justice in the Light of Judicial Reform in Ukraine: materials of the int. scient. and pract. conf. Yu.S. Chervonogo], Odessa, 18 December, Ukraine: National University "Odessa law academy", p. 75.

Each stage is recorded in the narrative part of the protocol, the results of the review (web-pages, photos, screenshots) are printed and filled to the protocol. In addition, the protocol describes the inspected web pages, the content of evidence, the place and time of the notarial action, information about the persons who are interested in, and the notary. That is, the notaries of Russian Federation make appropriate protocols, which do not require any legalization. They are translated into Ukrainian and submitted to court as evidence. However, this method takes a lot of time.

Taking into account the existence of the problem of certification of electronic copies of electronic evidence, there is a need to amend the Law of Ukraine *On Notary*, adding in Art. 34 "Notarial Acts Performed by Notaries", the following provisions:

"certify the fidelity of electronic and paper copies of electronic documents".

It seems appropriate that in order to solve the problem regarding notarization of web-screenshots, it is necessary to develop a remote system of automated notarization of copies of the Internet pages, websites and data in the Internet at a certain point in time, which will be the same for all EU countries and, in particular, for Ukraine.

Providing of such remote system of automated notarization is possible with the following algorithm:

- 1) identification of the Internet resource, which has a destructive character, making a decision on fixing the content and certifying it notariially;
- 2) choosing in the special online resource (e.g. for Ukraine – the online resource of Ministry of Justice of Ukraine) the necessary type of remote automated notarization of information posted on the Internet;
- 3) filing online application for notarization of Internet pages with the data on: the address (URL) of the web-resource, which contains data that the user intends to certify notariially; personal data of the customer services (first name, last name, number and series of passport, e-mail, etc.);
- 4) on-line fulfilment of the application for notarization of information placed on the Internet, by its processing by a special automated software and hardware complex

in automatic mode (verification of the accuracy of displaying the content of the site, displaying the main page, moving to the necessary pages, checking the domain name, determining DNS servers, checking the IP address matching, etc.);

- 5) providing the customer check-card with information on the fulfilment of the application (or the impossibility of the fulfilment) and individual order code in an automatic on-line regime;
- 6) payment of the service by the customer in accordance with the tariff;
- 7) obtaining by an individual order code at the notary (private or public) paper materials, certified by a notary's seal, or electronic materials, certified by an electronic digital signature of the notary.

Thus, the normalization and introduction of a common mechanism for notarization of information from the Internet will promote:

- 1) increasing of the responsibility of the Internet users for the reliability, truthfulness of information and data placed on the Internet;
- 2) reducing the level of trust in fake information (from unconfirmed sources);
- 3) significantly expanding the scope of legal instruments for the protection of the rights and freedoms of a citizen and state authorities from the dissemination of false and defamatory information, the illegal collection and dissemination of confidential information, personal data, etc.;
- 4) timely response of the state to challenges related to the dissemination of confidential and information of an extremist nature, illegal interference with the operation of state electronic information resources, unauthorized copying, modification, destruction or blocking of information processes in state electronic information resources.

Unfortunately, in judicial practice there are cases when the judge denied parties to provide evidence. Therefore, a person, if he (she) considers the actions of the court illegitimate, should have the right to apply

to the notary for providing evidence, as the shortcomings of the legislation of Ukraine may adversely affect his (her) rights. Thus, the *Pechersk District Court of Kiev* indicated that a simple screenshot, in which the web-page was opened in the browser window, and the printout of its contents are not valid and admissible evidence in this case (Decree of 1. 4. 2016 in case number 757/13905/16³⁰, Decision of 24. 5. 2017 in case number 757/43218/16³¹).

Thus, as was mentioned above, Ukraine currently does not have a well-defined mechanism for fixing information obtained from the Internet at a certain point in time. The implementation of this system, as an additional way of fixing such information, will expand the scope of information technology use in the judicial process, improve the process of providing notarial services, protect rights of participants of civil procedure and optimize the costs of both participants of the case and the state.

10. OTHER WAYS TO ENSURE ELECTRONIC EVIDENCE

Kalamaiko offers another way of extrajudicial ensuring of evidence, namely, access to independent organizations that provide services for fixing information on web pages. There are resources that allow taking a “snapshot” of information posted on a website at a certain point in time (*archive.is*, *peeps.us*). Such a file is saved on the server of the organization and placed in public access, so that the court can directly verify the existence of such information.³²

Also, there is an *Mayback Machine Internet Archive* (*archive.org*), an independent resource that saves copies of web pages at different times, depending on their popularity. It belongs to a non-profit organization and has the legal status of a library. Due to this, it is already actively used all over the world and its proven force was recognized by design in the case *Telewizja Polska USA, Inc. v. EchoStar Satellite* from 15. 10. 2004.³³

³⁰ Decision of Pechersk District Court of Kyiv from 1. 4. 2016 in case No 757/13905/16. [online] In Ukrainian. Available from: <http://www.reyestr.court.gov.ua/Review/56950422> [Accessed 17 January 2019].

³¹ Decision of Pechersk District Court of Kyiv from 24. 5. 2017 in case No 757/43218/16. [online] In Ukrainian. Available from: <http://www.reyestr.court.gov.ua/Review/66859813> [Accessed 17 January 2019].

³² Kalamayko, A. (2015) The Internet Network as a Source of Evidence in the Civil Process. *Yurydychna Ukraina. Civilnyi proces*, 4 (50), p. 120.

³³ *Ibid.*

Nowadays Ukrainian courts accept data from this independent resource as appropriate evidence. For example, in the decision of *Goloseevsky District Court of Kyiv* from 10. 10. 2015 in case No 752/9476/15, the Court explained why it trusts this source:

*“Snapshots of web-pages made with the help of online services for storing web-page content, are carried out using software hosted on the server of non-interested person. The corresponding file with the snapshot is also stored on the server of such person and placed in public access on the Internet. Together with the snapshot, the original web-page address and the exact time when it was made are recorded. In this case, the information that on a web-page is copied directly, instead of displaying it on the user’s screen. In this way, the possibility of modifying the original content of web-page is virtually eliminated, since all operations related to fixing content of web-page and its storage are carried out without interference by any interested parties”.*³⁴

However, there are certain technical limitations for fixing the contents of a web-page: objects larger than 10 MB in size are not saved; pages with restricted access are not saved also. In addition, at the request of the website owner, data from this web archive can be deleted.

Consequently, there are *several ways of investigation, fixation and certifying web-screenshots*:

- 1) inspection of evidence by the court at its location (review of the website, or other places of data storage on the Internet);
- 2) review and certification of the web-page by a notary;
- 3) use of *InternetArchive*, *WaybackMachine* services;
- 4) conducting an expert examination 10.17 – examination of telecommunication systems (equipment) and facilities.

There are other ways of fixing web-screenshots, however, the question of relevance and admissibility of such methods remains controversial.

The abovementioned rules for drawing up screenshots allow evaluating them as evidence in the case. A simple printout of the screenshot without reference of the date, time, website from which it was executed, without

³⁴ Decision of *Goloseevsky District Court of Kyiv* from 10. 10. 2015 in case No 752/9476/15. [online] In Ukrainian. Available from: <http://reyestr.court.gov.ua/Review/52726541> [Accessed 17 January 2019].

the signature and initials of the executor can not be considered as proper evidence.

Screenshots can be used with other evidence if they correspond all the requirements. When giving a screenshot as evidence, it is necessary to provide the following information:

- 1) time and date of the photo (to confirm the relevance of the information provided);
- 2) the address and the name of the photographed site;
- 3) the name, signature and position of the person who made the screenshot;
- 4) translation of information in a foreign language into Ukrainian;
- 5) notarization of the screenshot.

It is also important to save a screenshot of the web-page on computer's hard drive or on portable storage devices, which will ensure that such evidence can not be lost.

11. CONCLUSIONS

Electronic forms of communication, first of all, social networks and the Internet, have reached great level of influence on public life, so they became an important source of information, and therefore there is a need of normative settlement of its using in the process of resolving of civil cases by a court.

Summarizing, we must state that in practice many questions arise about the possibility of using information from websites as evidence. Normative regulation of electronic evidence provided by the current Ukrainian legislation is limited and does not allow the participants to fully realize their obligation to prove all the circumstances on which they refer to both their claims and objections, as well as their rights on effective judicial protection, guaranteed the Constitution of Ukraine and the European Convention on Human Rights.

In the context of the ever-increasing use of various information technologies in public relations, electronic correspondence, the emergence and rapid development of e-commerce, electronic means of payment, there is a need for a normative regulation of the use of web-screenshots as a means of proof in civil procedure.

Screenshots contain information about the facts on the basis of which the court can establish: the circumstances on which arguments of parties are based; presence or absence of violation; guilt and other circumstances relevant to the case. Thus, screenshots can serve as evidence in court during consideration of civil cases, however, they must be drawn up and issued in a documented order.

It seems appropriate to regulate on legislative level a list of ways of fixing the information, placed on the Internet, accessible to the participants of the case. It is proposed to expand their capabilities by providing notaries with a separate authority regarding certification of such evidence, which in practice will help to avoid collisions, as well as filling the existing gaps in the legislation regarding electronic evidence.

The only way to resolve this problem is adopting amendments to the current CPC of Ukraine, creating a remote system of automated notarization of copies of the Internet pages, websites and data on the Internet at a certain point in time, which will be the same for all EU countries and establishing obligation for the Internet providers to keep information placed on their electronic resources [within one year (as it is legally established for appealing to a court with a claim of refutation inaccurate information that was posted in the media)]. But, nonetheless, it should not be forgotten that Ukrainian legislation emphasizes that personal information can only be extracted in individual cases in special order.

LIST OF REFERENCES

- [1] Afyan, A. (2013) The role of the notary in the process of proving the facts regarding information in the Internet. *Civilisticheskaya processualnaya musul'. Mezhdunarodnyi zbornik nauchnykh statey*, 2.
- [2] Badila, O. (2014) Evidence and the need to provide them with a notary and a court: topical issues. *Nashe pravo*, 4.
- [3] Decision of Goloseevsky District Court of Kyiv from 10. 10. 2015 in case No 752/9476/15. [online] In Ukrainian. Available from: <http://reyestr.court.gov.ua/Review/52726541> [Accessed 17 January 2019].
- [4] Decision of Pechersk District Court of Kyiv from 1. 4. 2016 in case No 757/13905/16. [online] In Ukrainian. Available from: <http://www.reyestr.court.gov.ua/Review/56950422> [Accessed 17 January 2019].

- [5] Decision of Pechersk District Court of Kyiv from 24. 5. 2017 in case No 757/43218/16. [online] In Ukrainian. Available from: <http://www.reyestr.court.gov.ua/Review/66859813> [Accessed 17 January 2019].
- [6] Decision of the High Specialized Court of Ukraine for the consideration of civil and criminal cases from 22. 2. 2017, Case No 761/13156/16-п. [online] Available from: <http://www.reyestr.court.gov.ua/Review/65038960> [Accessed 17 January 2019].
- [7] Directive 1999/93/EC of European Parliament and of Council of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive). *Official Journal of European Communities*. L 13. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093> [Accessed 17 January 2019].
- [8] Directive 2000/31/EC of European Parliament and of Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in Internal Market (Directive on electronic commerce). *Official Journal of European Communities*. L 178. [online] Available from: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031> [Accessed 17 January 2019].
- [9] Draft Law on Amendments to Article 100 of Civil Procedural Code of Ukraine (regarding the certification of copies of electronic evidence). [online] Available from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63876 [Accessed 17 January 2019].
- [10] Fundamentals of the legislation of the Russian Federation on notary, Federal Law of 11. 2. 1993, No 4462-1. [online] In Russian. Available from: https://www.consultant.ru/document/cons_doc_LAW_1581 [Accessed 17 January 2019].
- [11] Chornyi S. and Antoniyuk O. (2018) Electronic evidence in civil proceedings: problems of practical application. *Visnyk students'kogo naukovogo tovarystva DonNU imeni Vasyl'ya Stusa*. [online] Available from: <http://jvestnik-sss.donnu.edu.ua/article/download/5468/5495> [Accessed 17 January 2019].
- [12] Kalamayko, A. (2015) The Internet Network as a Source of Evidence in Civil Process. *Yurydychna Ukraina. Civilnyi proces*, 4 (50).
- [13] Kucher, T. (2013) Features of the application of evidence created with the help of computer technologies in the notarial process. *Civilisticheskaya processual'naya musul'*. *Mezhdunarodnyi zbornik naychnukh statey*, 2.
- [14] Laz'ko, O. (2015) Prospects for the development of electronic (technical) means of proof in civil process of Ukraine. *Evropeyski perspektivy*, 1.
- [15] Lezhuh, T. (2013) The use of electronic evidence in cases relating to the protection of honor, dignity and business reputation. *Viche*, 16.

- [16] Minsk Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters (7. 10. 2002). [online] Available from: <http://cisarbitration.com/wp-content/uploads/2017/02/Minsk-Convention-on-Legal-Assistance-and-Legal-Relations-in-Civil-Family-and-Criminal-Matters-english.pdf> [Accessed 17 January 2019].
- [17] Okhromeev, Yu. (2012) Collection of evidence base in cases of violation of rights in the Internet. [online] Available from: http://uba.ua/documents/text/27_01_2012/Okhromeev.pdf [Accessed 17 January 2019].
- [18] Pavlova, Iu. (2017) Some aspects of the admissibility of electronic evidence in the civil procedural procedure law of Ukraine. *Prykarpatskyi yurydychnyi visnyk*, 5 (20).
- [19] Petrenko, V. (2018) Electronic evidence as an element of information technology in civil justice. *Molodyi vchenyi*, 1 (53).
- [20] Procedure for certifying the authenticity of copies of documents, Ukraine. [online] Available from: <http://www.minjust.gov.ua/15101> [Accessed 17 January 2019].
- [21] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of European Communities*. [online] Available from: <https://eur-lex.europa.eu/eli/reg/2014/910/oj> [Accessed 6 May 2019].
- [22] Reshetnikova, I. and Yarkov, V. (1999) *Grazhdanskoe pravo i grazhdanskiy process v sovremennoy Rossii* [Civil law and civil process in modern Russia]. Moscow: Izdatelstvo Norma.
- [23] Tripulskiy, G. (2015) Some aspects of the admissibility of evidence obtained on the Internet in the civil process. *Tsyvil'ne sudochynstvo u svitli sudovoi reformy v Ukraini: materialy mizhn. nauk.-pract. konf. im. Yu. S. Chervonogo* [Civil Justice in the Light of Judicial Reform in Ukraine: materials of the int. scient. and pract. conf. Yu.S. Chervonogo], Odessa, 18 December, Ukraine: National University "Odessa law academy".
- [24] Tripulskiy, G. (2015) The possibility to provide evidence in the case by notaries. *Tsyvil'ne Sudochynstvo u svitli sudovoi reformy v Ukraini: materialy „kruglogo stolu“* [Civil justice in the light of judicial reform in Ukraine: materials of the "round table"], Odessa, 16 May. Ukraine: National University "Odessa law academy".
- [25] Tsehan, D. (2013) Digital evidence: the concept, features and place in evidence system. *Naukovyi visnyk Mizhnarodnogo humanitarnogo universytety. Iurisprudencia*, 5.

- [26] U.S. Supreme Court, *Daubert v. Merrell Dow Pharmaceuticals Inc.*, United States Reports, vol. 509, 1983.
- [27] UNCITRAL Model Law on Electronic Commerce (1996). [online] Available from: https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf
[Accessed 17 January 2019].
- [28] UNCITRAL Model Law on Electronic Signatures (2001). [online] Available from: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf>
[Accessed 17 January 2019].
- [29] Yacenko, O. (2013) Providing evidence by notaries, or neighboring experience, which is lacking in Ukrainian lawyers. *Yurydychnyi zhurnal*, 5 (131).