ISSN 2308-0361

PROBLEMS OF IDENTIFICATION OF A COPYRIGHT INFRINGER FOR WORKS POSTED ON THE INTERNET

Kostiantyn Zerov,
postgraduate student of the Taras Shevchenko National University of Kyiv; junior researcher of Intellectual Property Research Institute of the NALS of Ukraine.

Зеров К. Проблеми ідентифікації особи-порушника авторського права на твори, розміщені в Інтернеті.

У публікації розглянуто проблеми ідентифікації особи — порушника авторських прав на твори, розміщені в мережі Інтернет. Автор класифікує таку ідентифікацію на види залежно від особливостей протиправної поведінки особи на: 1) ідентифікацію особи-власника веб-сайту; 2) ідентифікацію особи-користувача веб-сайту, що розмістив твір; 3) ідентифікацію особи-користувача P2P-мережі; кожна з яких має свої особливості. Проаналізовано, що процес ідентифікації особи, що вчинила пряме порушення авторських прав (користувача веб-сайту, що розмістив твір, та користувача P2P-мережі), поділяється на три стадії: 1) визначення і збирання IP-адрес; 2) знаходження відповідності IP-адреси визначеним абонентам (користувачам) окремих інтернет посередників; 3) інформування чи направлення претензій особам щодо порушення ними авторських прав та можливості подання (чи безпосередньо подання) проти них позовів. Автором зроблено висновок, що для ідентифікації особи-порушника (а не місця, дескоєно порушення) авторських прав на твори, розміщені в мережі Інтернет-виключно використання IP-адреси недостатньо, тому необхідно використовувати додаткові докази в сукупності для встановлення причинново-наслідкового зв'язку між особою-абонентом (кінцевим користувачем), якому делеговано певну IP-адресу, та порушенням авторського права.

Ключові слова: Інтернет, піратство, авторське право, ідентификація

Topicality. Problem of identification of an alleged infringer of copyright within the relative anonymity of Internet users remains pending and unsolved problem of copyright protection for works posted on the Internet. Without solving this issue it is almost impossible to determine the entity of appropriate legal relationship.

The relative anonymity of users has a dual meaning. On the one hand, such activity in some way contributes to copyright infringement. Ye. Mykhailenko emphasizes that the problem is the main source of negative phenomena on the Internet [1, 9]. However, as fairly noted by O. Pastukhov, such anonymity is not a specific problem of a copyright law, though it applies to all crimes and torts occurring through the Internet network [2, 57]. For example, distribution of pornographic works, the legal relationship associated with protection against defamation, combating terrorism and separatism manifestations indicate the systemic nature of specified problem. However, we shall note that anonymous character of connections does not prevent from socially useful actions at all (*e.g.*, legal distribution of works).

On the other hand, the issue of anonymous nature of Internet users shall be considered with the principle of proportionality of intellectual property rights

(as well as other rights that may be subject of infringing activity) and the right for freedom of expression, respect for private and family life. Thus, the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, which was presented to the UN Council on Human Rights at XXIX meeting (as of May 22, 2015) emphasized that encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age [3, clause 56].

Specified principle of proportionality shall not interfere with measures taken to search persons responsible for criminal acts under national law, the European Convention on protection of Human Rights and other fundamentals, and other international agreements in the field of justice and policing, as noted, in particular, in the «Declaration on freedom of communication on the Internet» of the Committee of EC Ministers [4].

The relevance of the specified problems concerns the fact that in copyright-based relations (as civil relations) proving of a causal connection between the unlawful conduct of the person and caused damage as one of conditions for liability on violation of intellectual property rights is vested upon the plaintiff, *i.e.,* copyright holder (or a person authorized to act on the holder's behalf).

Within this study the author **specified the objective** to analyze the main approaches to identification of the person — an alleged infringer of copyright for works posted on the Internet.

Analysis of key studies and publications. The indicated problems almost have not been studied within study of problems of intellectual property in Ukraine. Still, there are respective researches within information law field; specifically, M. Gutsaliuk paid attention to the introduction of ID-web as a prerequisite for the Internet security.V. Butuzov, V. Gavlovsky, V. Golubev, R. Kaliuzhny, V. Tsymbaliuk draw attention to the need of development the Information Code, building of appropriate institutional structures of law enforcement agencies to detect and investigate crimes related to the use of the Internet and etc. The issues of identification of users of social networks on the Internet involved S. Bartunov and A. Korshunov. The issue of identifying the end-users of the Internet in copyright legal relationship has been the subject of a number of studies of foreign authors, among which we can emphasize T. Harding, D. Goldschlag, M. Reed, P. Syverson, M. Robert Filby, and M. Piatek.

Summary of basic material. In our opinion, problem of identification of a person — infringer of copyright for works posted on the Internet — at the logical level of the Internet network structure* shall indicatively considered depending on kinds of the illegal behaviour of a person.

1. Identification of a person — owner of the website.

2. Identification of a person — user of the website who posted the work.

3. Identification of a person — user of the P2P network.

Each of the above situations has own characteristics, which are discussed below.

As of May 2016 in Ukraine the possibility to identify an individual — an infringer of copyright for works posted on the Internet within the civil protection is provided only within the judicial form of protection, namely in accordance with part 1 article 133 of the Civil Procedure Code of Ukraine for the person (hereinafter — the CPC of Ukraine), through evidence provision. In accordance with

* The author shares the approach proposed by J. Benkler; according to which there are defined the following hierarchical levels of information environment: level of content (information available to be viewed by a user); logic level (regulation of software, Internet protocols) and physical layer (hardware both of users and Internet service providers) [5, 561–563].

part 1 article 134 of the CPC of Ukraine, the statement on evidence provision shall contain the following: evidence subject to provision; circumstances to be substantiated by the evidence; circumstances indicating that provision of required evidence may be impossible or complicated, and case that requires the evidence or the purpose of their provision [6]. The specified institution is used mostly for «domain disputes» to identify the registrant of the domain name*.

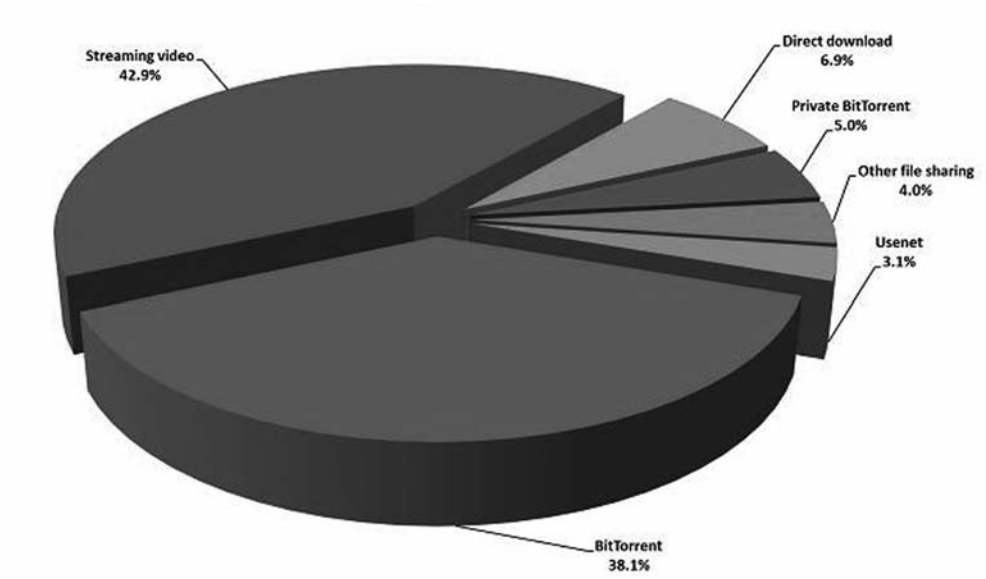
The draft law «On amendments to some legislative acts of Ukraine on protection of copyright and related rights on the Internet» as of May 10, 2016 № 4629 specifies provision of the copyright holder with an opportunity to receive the following:

1) from the owner of the website - information that identifies a user of the website, who, according to the entity possessing copyright and (or) related rights or its authorized representative, has posted on the website information violating the copyright and (or) related rights, and under condition of availability of contact details of the userof the website, required to send a petition to the court to consider the dispute in the court concerning illegality of the actions of such user at posting information on the website;
2) from the hosting service provider - information that identifies the owner of the website, using hosting services of the provider to host and provide access to information, that according to the copyright and (or) related rights, violates copyright and (or) related rights, and contact information required to send a petition to the court to consider the dispute in the court concerning illegality of the actions of such owner of the web site [7, article 52-2].

We shall note that owner of the website in accordance with the provisions of the draft law № 4629 is recognized by domain name registrant or other person who defines the procedure and conditions for use of the website and (or) procedure of information posted there. In author's opinion, such approach is justified, becauses it is unconditionally imprudent to equate the website owner and domain name registrant, since the legal nature of a website relates to copyright and domain name delegation relates to the contractual relationship; the registrant of the domain name is not necessarily the same person as the owner of the website (for example, contract on the use of the domain name has been concluded).

The problem of identification of the owner of the website through a domain name registrant is the subject to be solved by ICANN at self-regulation level. Thus in December 2015 the GNSO council of ICANN adopted recommendations «Illustrative Disclosure Framework», which provisions offer the procedure of receipt of information by the copyright holders about registrants of domain names (suspected of piracy), stored in a WHOIS — base from proxy — and privacy registrars accredited by ICANN. In addition, the registrar cannot refusethecopyright holderas for disclosure of such information because of the lack of a judgment, court summons, a civil suit or arbitration of the domain dispute according to the UDRP or URS procedures. Moreover, refusal to disclose information about the registrant cannot be based solely on the fact that the request relates to infringement of intellectual property by objectsposted on such website, not to the domain name. The registrar of such domain name shall be notified about a complaint and within 15 days may either abandon the domain name, or provide evidence of them being uninvolved to in-

* However, if the website is in domain zone .ua it is enough to see the field «license» in WHOIS-service to identify the registrant. The value of this field corresponds to the certificate of Ukraine for trademarks and services.



Picture 1. Estimate of online piracy methods, March 2016 by number of users

fringements of intellectual property, referred to in the complaint. If they prove convincingly, access will be denied to personal information of the registrant of the domain name [8].

However, in the draft law № 4629 the problems of identification of a person who is the user of P2P-network (direct infringer of copyright) are not taken into account, what, in our opinion, is a significant drawback. Thus, according to the MPPA, in March 2016 copyright infringement via P2P-networks accounted to 38.1 % of the total number of infringement of copyright for the works posted on the Internet *(see the picture above)* [9].

The process of identification of the person who committed direct copyright infringement (user of website who posted the work and user of P2P network) in foreign scientific literature is usually divided into three stages [10, 36, 37].

The first stage consists of actions of the copyright holder (or a person authorized to act on the holder's behalf) in order to identify and collect IP-addresses (numerical sequence that serves as an identifier of the Internet-server [11]). Without IP-address the user can neither send nor receive packets of data and other information useful for identification ofan alleged infringer.

The copyright holders use the following methods to identify and collect IP-addresses of infringers ofcopyright within operation of P2P networks:

- Indirect identification of users, based on a set of data about peers, returning from torrenttrackers.
- Direct identification of users. According to Tom Harding, is based on connection with a torrent tracker to users distributing certain files and further exchange of files with them. Direct identification looks to demonstrate that users are actually engaging in the file sharing [12, 8].

Both methods do not exclude the possibility of errors and mistakes. Thus, according to research by American scientists M. Piatek, T. Kohno and A. Krishnamurthy, any Internet user can get a warning for copyright infringement because of an artificial substitution of IP-address. Researchers received hundreds of actual reports on copyright infringe-

ment under DMCA law for computers and devices (including network printers) which have never been used (and could never been used) for spreading dissemination of works on the Internet [13, 7].

In addition, there are certain technical features that allow end-users to complicate their identification, while both of the above methods provide that users connect to the torrent server using IP addresses delegated personally to them. For example:

1) use of VPN or PROXY servers. In addition, such services are generally subject to foreign law and do not keep log files [10, 92] (files, containing information about time, actions and connections of certain persons);
2) D. Goldschlag, M. Reed, P. Syverson and M. Filby also note the possibility of usingDarknet (Onion Routing / TOR) *i.e.*, a sequence of intermediate networknodes with encryption of transmitted information [14; 10, 93].

However, we shall note that there are technical means by which we can detect the actual IP address of the user, even such user uses TOR browser [15], but it seems extremely complicated to use such means in private legal relations.

3) also, according to Michael Piatek, users of P2P- networks use «blacklists» of known IP-addresses of copyright holders (or their representatives) to prevent from such monitoring [13, 4; 10, 95].

The second stage of identification is to establish the matching of IP-address to certain subscribers (users) of certain Internet intermediaries.

Foreign jurisprudence applies different approaches to solve the specified issue.

According to a research by S. B. Karunaratne, for judicial practice in the USA, since 2003, the copyright holders applysubpoenas to an Internet intermediary for identification of an alleged infringer to protect against copyright infringement of works posted on the Internet via torrent trackers (so-called «John Doe» in the countries of the Anglo-Saxon law) — users of Bittorent trackers involving Internet intermediaries for further identification of such users [16, 284–288; 17]. In some cases the number of respondents totalled more than 2 000 [18]. In addition, according to the provisions of paragraph 5 part (h) § 512 of the DMCA law the Internet intermediary shall expeditiously disclose to the copyright holder or person authorized by the copyright holder the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification [19].

In the UK, in order to match the IP-address of a person the Norwich procedure is applied (it was first used in patent case of Norwich Pharmacal Co. against Customs and Excise Commissioners [20]), which is a court order for disclosure of documents or information available to the third party regarding the identity of an allegedinfringer of intellectual property rights. Adoption of the Digital Economy Act (DEA) in 2010 [21] specified a special procedure of informing of the Internet intermediary by the copyright holder about online copyright infringement (copyright infringement report, CIR); procedure of notification about received complaints performed by the Internet intermediary towards its user; procedure to provide a list of infringers to the copyright holder (copyright infringement list, CIL). In addition, the specified list under the provisions of article 124 — under DEA law *shall not contain information that directly identifies the user*. Only after specified actions the copyright holder may apply for receipt of the order of Norwich.

According to provisions of article 15 of Directive 2000/31/EU «On electronic commerce» the Internet intermediaries are charged neither with general obligation to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. However, national legislation of EU Member States may establish obligations

for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements [22, article 15].

From 2006 to 2014 there was in force the EU Directive 2006/24/EU «On the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks» [23], provisions of which were applied to traffic and data about location of both legal entities and individuals, as well as relevant data necessary to identify the subscriber or registered user. According to provisions of articles 5 and 6 of this Directive, the Internet intermediaries kept, in particular, information about access to the Internet, e-mail and Internet telephony: date and time of connection and disconnection of access to the Internet with the IP-address assigned by the provider of access to the Internet as well as ID of the subscriber or registered user; date and time of connection and disconnection of the service of email, over the Internet, or Internet telephony. However, they have to be kept for at least six months and not more than two years. Such information was provided upon the request of state authorities.

However, the European Court of Justice within the joint case of C-293/12 and C-594/12 admitted the specified Directive void from the date of its adoption, as its provisions interfered in a particularly serious manner with the fundamental rights of humans and citizens:the right for freedom of expression, respect for private life and the right for personal data protection [24].

In 2010 there was adopted the Law of Ukraine № 1819-VI «On Amendments to Certain Legislative Acts of Ukraine on combating the spread of child pornography» which introduced amendments to the Law «On Telecommunications», in particular part 2 article 39 «The operators, telecommunication providers keep and provide information aboutconnection of its subscriber in the manner prescribed by legislation». In addition, pursuant to the provisions of parts 1 and 3 of article 34 of the specified law, the telecommunication operators and service providers are obliged to provide and be responsible for the safety of information about the user received at the conclusion of the contract, provided telecommunication services, including receipt of services, their duration, subject, route of transmission, etc. [25]. Regarding the above mentioned, following shall be emphasized:

First, the above provisions shall be considered within system connection with part 2 of article 32 of the Constitution of Ukraine, according to which the collection, storage, use and dissemination of confidential information about a person without its consent are not allowed, except in cases specified by law, and only for interests of national security, economic prosperity and human rights.

Second, there is no special lawful procedure concerning demanding information about connections of the subscriber from Internet intermediary under civil law protection as of May 2016 (there are only general provisions for evidence provision in accordance with part1 of article 133 of the CPC of Ukraine; collection of evidence in case of criminal proceedings or investigative proceedings (article93 of the Criminal Procedural Code of Ukraine, clause6, part 1 of article 8 of the Law of Ukraine «On Operative Investigation Activities»), the draft № 4529 also does not specify such procedure. In our opinion, the legislation of Ukraine shall include a procedure for the possibility of extra judicial claiming of the copyright holder (or a person authorized to act on the holder's behalf) to an Internet intermediary with the requirement to

provide a list of infringers of copyright — subscribers of such intermediary, taking into account the principle of proportionality, specifying the list of information required for filing such claim and liability for such information misuse.

In addition, it seems necessary to point out certain features of this stage in Ukraine. According to article 24 of the Rules on provision and obtaining of telecommunication services,approved by the Cabinet of Ministers of Ukraine as of April 11, 2012 № 295 (hereinafter referred to as the Rules) [26], while connecting terminal equipment of the user to telecommunication network the operator shall assign it a number or other network identifier (unique sequence of numbers and/or symbols assigned to the subscriber's terminal equipment and/or user in the telecommunication network or the Internet); and/or apply the personal number of the subscriber. However, these Rules do not specify the obligation of the Internet intermediary to provide «external» unique identifier (IP-address). According to some rate plans of certain Ukrainian Internet intermediaries the allocation of fixed static IP-address is optional paid service.That is in relation to the outside world such end-users can have the same IP-address — the IP-address of Internet intermediary — it extremely complicates matching of certain IP-address and certain subscribers (end-users) of such Internet intermediaries. For that matter it is appropriate to provide in the Rules the duty of telecommunication operator to assign to its subscribers «external» fixed static network ID.

The third stage is to inform or send claims to persons as for infringement of copyrights by them and the possibility of filing (or direct filing) of claims against them.

As noted by M. Filby, this stage is the most complicated because it requires evidence for two components, namely:the establishing of a connection between person — subscriber of the Internet intermediary and the infringement, and proving that the IP-address has in fact participated in unauthorized distribution of works to a legally significant degree [10, 40].

In our opinion, certain caution shall be ensured with respect to identification of a person — infringer of copyright exclusively by IP address because IP address provides information only about the source of connection — a particular place (not the person), using which the uncertain number of hardware can connect to the Internet. For example, mailbox or telephone number may also be used by unspecified number of users.

Also an additional problem for end-users' identification by IP-address is the active development of the Internet of things. Thus, various stationary devices with an access to the Internet can make connections to the network offline, without participation of individuals themselves. Identification of the person who could program the respective devices for illegal activity scenarios, according to the author, is even more difficult task than to identify the person accessing the Internet in «normal» mode.

Foreign experience shows that courts in foreign countries also pay attention to the examined problem:

In the UK the England and Wales High Court considering case of Golden Eyeand others against Telefonica [2012] EWHC 723 (Ch) specified that subscriber with certain delegated IP-address was not necessarily the person who participated in the infringement of the copyright using P2P-network. There is a number of alternatives, including:

- the IP-address identifies a computer and someone else in the same household (whether a resident or visitor) was using the computer at the relevant time (which might be with or without the knowledge of the subscriber);
- the IP-address identifies a router and someone else in the same household (whether a resident or visitor) was using a computer communicating via the same router (which might be with or without the knowledge of the subscriber);

- the IP-address identifies a wireless router with an insecure (either open or weakly encrypted) connection and someone outside the household was accessing the Internet via that router (in all probability, without the knowledge of the subscriber);
- the IP-address identifies a computer or router, the computer or a computer connected to the router that has been infected by a Trojan and someone outside the household was using the computer to access the Internet (almost certainly, without the knowledge of the subscriber);
- the IP-address identifies a computer-which is available for public use, for example in an Internet cafe or library [27, clause 103].

In the USA, for case of K-Beech, Inc. against John Does 1-37 (CV 11-3995 (DRH)(GRB) the District Court of Eastern District of New York concluded that some IP-addresses could be delegated to organizations providing Internet access to their employees, clients or uncertain members (library, cafe) [28, 6–7].

In this regard it shall be noted that IP-address is not the only possible ID of the user of the Internet. In particular, there is a MAC-address in addition to IP-address. While the IP-address can provide information about the location, the MAC-address is a unique hardware address for each unit which is connected to the Internet [29]. In this case, one IP-address can at the same time have only one correspondent MAC-address of the device connected to the Internet, such as router of the user (indicated the technical information is available at information intermediaries). MAC-addresses of certain devices connecting the router are usually not stored, that is a problem for public use networks. In addition, the MAC-address, as well as the IP-address, can be technically changed.

Additional evidence required to confirm identification of a person-infringer of copyright, in addition to IP and MAC-address, can include, for example, the conclusions of a comprehensive examination (computer and technical expertise and intellectual property items) as for availability of respective copies of works on hardware of persons-infringers of copyright that is confirmed with materials of Ukrainian court practice in the article176 of the Criminal Code of Ukraine [30].

Conclusions

1. Performed study indicates the absence of effective, reliable and prompt mechanism of identification in the current actual legal regulation of the person violating copyright for works postedon the Internet.

2. Identification of aperson-infringer of copyright as for works posted on the Internet can be indicatively considered depending on the characteristics of unlawful behaviour of a person: 1) identification of the person-the owner of the website; 2) identification of the person-the user of the website where the work was posted; 3) identification of the user of P2P network

3. The process of identification of the person who committed direct copyright infringement (the user of the website who posted the work and user of P2P network) is usually divided into three stages: 1) identification and collection of IP-addresses; 2) detection of correspondence of the IP-addresses of to the specified subscribers (users) of certain Internet intermediaries; 3) informing or sending claims to individuals regarding infringement of copyright and the possibility of filing (or direct filing) of claims against them.

4. In the decree of the Cabinet of Ministers of Ukraine «On approval of rules of provision and receipt of telecommunication services» dd. April 11, 2012 No. 295 it is appropriate to specify the duty of the telecommunication operator to assign to its subscribers the «external» fixed static network ID, as far as the procedure of allocation of fixed static IP-address as additional paid service significantly complicates detection of correspondence of IP-address to certain subscribers (end-users) of such Internet intermediaries.

5. Use of IP-address only is not enough for identification of the persons-infringers of copyright (rather than the place where the infringement is committed) for works posted on the Internet, thus it is necessary to use additional evidence to establish a causal connection between the person-subscriber (end-user), with certain delegated IP address, and copyright infringement. ♦

Список використаних джерел / List of references

1. *Михайленко Е. В. Проблемы Информационно-правового регулирования отношений в глобальной компьютерной сети Интернет : автореф. дис. на соиск.уч. степени канд. юр. наук : спец. 12.00.14 «административное право, финансовое право, информационное право» / Михайленко Евгений Владиславович — М., 2004. — 25 с.*

Mihajlenko Ye. V. Problemy Informacionno-pravovogo regulirovanija otnoshenij v global'noj komp'juternoj seti Internet : avtoref. dis., M., 2004, 25 s.

2. *Пастухов О. М. Авторське право у сфері функціонування всесвітньої інформаційної мережі Інтернет : дис. канд. юр. наук : 12.00.03 / Пастухов Олександр Миколайович — К., 2002. — 173 с.*

Pastukhov O. M. Avtorske pravo u sferi funktsionuvannia vsesvitnoi informatsiinoi merezhi Internet : dys., K., 2002, 173 p.

3. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression[Electronic resource]. — Access mode : http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.*
4. *Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies) [Electronic resource]. — Access mode : http://www.osce.org/fom/31507?download=true.*
5. *Benkler Y. From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access / Yochai Benkler // Federal Communications Law Journal. — 2000. — № 52. — P. 561–579.*
6. *Civil Procedure Code of Ukraine from 18.03.2004 № 1618-IV // Vidomosti Verhovnoyi Rady, 2004, № 40–41, 42, Art. 492 (with amendments).*
7. *The draft law of Ukraine «On amendments to some legislative acts of Ukraine on protection of copyright and related rights on the Internet» № 4629 from 10.05.2016 [Electronic resource]. — Access mode : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59024.*
8. *Final Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process [Electronic resource]. — Access mode : http://gnso.icann.org/en/issues/raa/ppsai-final-07dec15-en.pdf.*
9. *Ukrainian Anti-Piracy Association / Internet piracy [Electronic resource]. — Access mode : http://apo.kiev.ua/internet.phtml.*
10. *Filby M. Regulating File Sharing: Using Law, Internet Architecture, Markets and Norms to Manage the Non-Commercial Sharing of Digital Information / M. Filby. — Lexington, KY, USA, 2015. — 248 p.*
11. *Ip address. (n.d.). The American Heritage® Science Dictionary [Electronic resource]. — Access mode: http://dictionary.reference.com/browse/ip address.*
12. *Harding T. BitTorrent tracking as a means of detecting illegal file-sharing / Tom Harding // E-Commerce Law & Policy — 2013. — № 2. — P. 08–09.*

13. *Piatek M. Challenges and Directions for Monitoring P2P File Sharing Networks — or — Why My Printer Received a DMCA Takedown Notice [Electronic resource] / M. Piatek, T. Kohno, A. Krishnamurthy — Access mode : http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf.*
14. *Goldschlag D. Onion Routing for Anonymous and Private Internet Connections [Electronic resource]/ D. Goldschlag, M. Reed, P. Syverson — Access mode : http://www.onion-router.net/Publications/CACM-1999.pdf.*
15. *Judge Confirms Carnegie Mellon Hacked Tor and Provided Info to FBI [Electronic resource]. — Access mode : http://gizmodo.com/judge-confirms-carnegie-mellon-hacked-tor-and-provided-1761191933.*
16. *Karunaratne S. The Case Against Combating BitTorrent Piracy Through Mass John Doe Copyright Infringement Lawsuits / Sean B. Karunaratne // Michigan Law Review. — 2012. — №111:283. — P. 283–309.*
17. *Borland J. RIAA sues 261 file swappers [Electronic resource]. — Access mode : http://www.cnet.com/news/riaa-sues-261-file-swappers/.*
18. *United States District court Northern district of California San Jose division. Case №: 10-CV-5865-PSG. Diabolic video productions, inc. V. Does 1-2099 [Electronic resource]. — Access mode: http://cases.justia.com/federal/district-courts/california/candce/5:2010cv05865/235553/16/0.pdf?ts=1428874690.*
19. *Digital millennium copyright act Oct. 28, 1998 [H.R. 2281] [Electronic resource]. — Access mode : https://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf.*
20. *Norwich Pharmacal Co v Customs and Excise Commissioners [1973] UKHL 6 (26.06.1973) [Electronic resource]. — Access mode : http://www.bailii.org/uk/cases/UKHL/1973/6.html.*
21. *Digital Economy Act 2010 CHAPTER 24 [Electronic resource]. — Access mode : http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf.*
22. *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [Electronic resource]. — Access mode: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32000L0031.*
23. *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [Electronic resource]. — Access mode http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.*
24. *Court of Justice of the European Union press release № 54/14 Luxembourg, 08.04.2014 Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others [Electronic resource]. — Access mode : http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.*
25. *The Law of Ukraine»Onamendments to severallegislative acts of Ukraine on combating the spread of child pornography» from 20.01.2010 № 1819-VI. // Vidomosti Verhovnoyi Rady — 12.03.2010 — № 10. — Art.105.*
26. *The Decree of the Cabinet of Ministers of Ukraine «On approval of rules of provision and receipt of telecommunication services» from April 11, 2012 № 295.// Uriadovyi kurier. — 2012. — № 109 (with amendments).*
27. *Golden Eye (International) Ltd & Anor v Telefonica UK Ltd [2012] EWHC 723 (Ch) (26.03.2012) [Electronic resource]. — Access mode : http://www.bailii.org/ew/cases/EWHC/Ch/2012/723.html.*
28. *K-Beech, Inc. v. John Does 1-37, CV 11-3995 (DRH)(GRB) [Electronic resource]. — Access mode : http://www.technollama.co.uk/wp-content/uploads/2012/*

05/92100289-K-Beech-Order-amp-Report-amp-Recommendation-Ordered-5-1-12.pdf.

29. *Mac address. Dictionary.com. The Free On-line Dictionary of Computing. Denis Howe. [Electronic resource]. — Access mode : http://dictionary.reference.com/browse/mac address (accessed: January 09, 2016).*
30. *The sentence of the Nakhimov District Court of Sevastopol on the case № 765/3456/13-к from 11.09.2013 [Electronic resource]. — Access mode : http://reyestr.court.gov.ua/Review/33485818.*

Надійшла до редакції 29.05.2016 р.

Зеров К. Проблемы идентификации лица — нарушителя авторского права на произведения, размещенные в Интернет. В публикации рассмотрены проблемы идентификации пользователя — нарушителя авторских прав на произведения, размещенные в сети Интернет. Автор классифицирует такую идентификацию на виды в зависимости от особенностей противоправного поведения лица на: 1) идентификацию лица — произведение; 3) идентификацию лица — пользователя P2P-сети; каждая из которых имеет свои особенности. Проанализировано, что процесс идентификации лица, совершившего прямое нарушение авторских прав (пользователя сайта, разместившего произведение, и пользователя P2P-сети), делится на три стадии: 1) определение и сбор IP-адресов; 2) нахождение соответствия IP-адреса определенным абонентам (пользователям) отдельных интернет посредников; 3) информирование или направление претензий лицам о нарушении ими авторских прав и возможности представления (или непосредственно представления) против них исков. Автором сделан вывод, что для идентификации личности — нарушителя (а не места, где совершено нарушение) авторских прав на произведения, размещенные в сети Интернет-только использование IP-адреса недостаточно, поэтому необходимо использовать дополнительные доказательства в совокупности для установления причинно-следственной связи между лицом-абонентом (конечным пользователем), которому делегирован определенный IP-адрес, и нарушением авторского права.

Ключевые слова: Интернет, пиратство, авторское право, идентификация

Zerov K. Problems of identification of a copyright infringer for works posted on the Internet. This publication examines the problems of identification of an alleged infringer of copyright for works posted on the Internet. The author divides types of such identification depending on the characteristics of wrongful conduct on the person: 1) identification of the person — the owner of the website; 2) identification of the person — the user of the website where the work was posted; 3) identification of the user of P2P network, where each has its own characteristics. According to analysis, the process of identification of the person who committed direct copyright infringement (the user of the website who posted the work and user of P2P network) is usually divided into three stages: 1) identification and collection of IP-addresses; 2) detection of correspondence of the IP-addresses of to the specified subscribers (users) of certain Internet intermediaries; 3) informing or sending claims to individuals regarding infringement of copyright and the possibility of filing (or direct filing) of claims against them. The author concludes that use of IP-address only is not enough for identification of a person — infringer of copyright (rather than the place where the infringement is committed) for works posted on the Internet, thus it is necessary to use additional evidence to establish a causal connection between the person — subscriber (end-user), with certain delegated IP-address, and copyright infringement.

Keywords: Internet, piracy, copyright, identification