УДК 343.7
DOI: 10.31733/2078-3566-2020-2-35-41

Gulnaz A. RZAYEVA©
PhD in Law
(the Baku State University, Azerbaijan)

PROTECTION OF HUMAN RIGHTS VIOLATED BY CYBERCRIMES IN GLOBAL INFORMATION SOCIETY

Гульназа Рзаєва. Захист прав людини, порушених внаслідок кіберзлочинів у глобальному інформаційному суспільстві. Глобальне інформаційне суспільство сформувалося в результаті глобалізації економічних, політичних, глобальних та інших відносин, що відбуваються по всьому світу, особливо після створення єдиної мережі Інтернет. Отже, зміни в суспільстві вплинули на методи порушення прав людини. Злочинці вже здійснюють свою незаконну діяльність у більш легкі і зручні способи. Це підтверджує актуальність проблеми «кіберзлочинність».

У статті аналізуються поняття «кіберзлочинність», «віртуальний простір» тощо, уточнюється відмінність між ними. Аналізуючи різні правові та теоретичні підходи, автор доходить висновку, що як «кіберзлочинність», так і «віртуальний простір» є як абстрактними, так і синонімічними термінами. Концепція віртуального простору застосовується, коли йде про технічні та управлінські аспекти, а кіберпростір використовується з соціально-гуманітарної позиції.

У статті свобода висловлювань особливо підкреслена серед прав, які є предметом кіберзлочинів. Якщо, з одного боку, свобода висльовлювань обмежена через відсутність доступності чи іншої цензури, з іншого боку, зловживання свободою висловлювань порушує права і свободи іншої особи. Злочини, вчинені шляхом реалізації свободи висльовлювань, умовно поділяються на дві групи, в обидва їх типи були проаналізовані автором і відзначені різні особливості.

У статті заходи щодо попередження кіберзлочинності традиційно поділяються на загальні і конкретні. Спеціальні заходи включають культуру глобальної кібербезпеки, а загальні заходи визначені в контексті інформаційної політики держави. У статті ретельно проаналізовано ці заходи та були висунуті відповіднірекомендації.

Problem statement. Rapid development of global information society led to a worldwide discussion of mechanisms for the protection of human rights, as well as struggle against violations. Global information society is a new type of society, where information circulation does not recognize time, space and political boundaries and fundamental decisions can be made to improve society in all aspects as a result of knowledge processing. Today Internet become an integral part of our lives, since main requirement of this society is to ensure everyone's participation in exchange of information. Committing illegal actions is also inevitable, along with the purposeful use of ICT capabilities. Even new ways of committing crimes existent in the traditional society were formed in cyberspace, that raised the issue of "cybercrimes". In the early stages of information society, cybercrimes focused only on information rights, but crimes committed today using ICT violate various human rights. This makes it necessary to strengthen struggle against cybercrimes at both international and national levels.

The article's objective is to analyze the notions "cyberspace" and "virtual space", to determine violations of personal privacy, intellectual property rights and other freedoms, to put forward suggestions about protection of human rights violated by cybercrimes.

Basic content. Cyberspace, or virtual space? The globalization of information society led to the emergence of the term "*cyberspace"*. The concept of "cyberspace" was first used in William Gibson's work "Burning Chrome" [7] in 1982 and later in "Neuromancer" [8] work in 1984.

According to the US Supreme Court concept, "Cyberspace is a unique tool that does not have a specific area, but open and accessible to anyone in any point of the world through

ORCID iD: https://orcid.org/0000-0001-5305-7113
gulnazaydin@yahoo.com

Internet". Commenting on "international space theory", Darrel Ment writes that there are three such places: Antarctic, outer space and the open sea. The author notes that the fourth such space is cyberspace and emphasizes that state sovereignty does not apply to this space [3, p. 70]. It is interesting that, a researcher exploring jurisdiction issues in cyberspace explains only the sides of copyright and slander [3, p. 97-101]. Such a question arises: If cyberspace does not include sovereignty of any state, how legitimate would it be if a state's law prohibits the posting of any information on Internet? Or can the state limit its citizens' access to any information? – The principles which cyberspace is based to answer all such questions, must have regulatory support. It is no coincidence that, states noted political, regulatory and networking support as a necessary measure for the further development of ICT in Okinawa Charter on the Global Information Society, adopted by "Great Eight" states on July 22, 2000.

Speeches on independence of cyberspace are sounded in modern times. For example, John Perry Barlow, the founder of the Electronic Frontier Foundation announced his famous Declaration on "Independence of Cyberspace" at Davos forum in 1996. The declaration addresses all states in this way: "Cyberspace does not concern your borders. Don't think you created it. Cyberspace is a public project. You have no place among us. You do not have superior authority in cyberspace. You have neither moral rights, nor coercion to dominate over us. We will create more fair and humanistic society than yours in cyberspace...[21]" Despite these speeches, cyberspace issues are still resolved within each state's jurisdiction. International law norms and principles are taken into account in this case.

In order to analyze the notion of "cyberspace", it is expedient to clarify the content of such terms like "information space", "Internet" and to distinguish between them. ***Internet*** is a worldwide system of computer networks designed to store and transmit information. That is why Internet is often referred to "global network", "worldwide network". This network cannot be identified with cyberspace. Darrel Ment writes that, we know where the Internet starts, but we can not define the boundaries of cyberspace and the point of its start. Therefore, the concept of cyberspace cannot be identified with concept Internet [3, p. 69-70]. The researcher's position can be considered acceptable, i.e. cyberspace – should be regarded as metaphorical abstract, virtual reality unlike Internet, which is a single computer network system. In short, cyberspace is an invisible "world" within global computer network.

Therefore, the concept **"***virtual space***"** is often used to characterize this world. The point is that, international law refers the concept "cyberspace" as a legal term. However, the term "virtual" can be found in many regulatory acts in national law. Based on the content of these statutory acts, we can say that, "virtual" in domestic law is understood as the relations established through Internet. Web sites like Virtual Azerbaijan [18], Virtual Karabakh [20] and others were created and operate. Moreover, the measures on expansion of promotion and spread of Azerbaijani realities in virtual world in State Program for 2016-2020 on "Implementation of the National Strategy for the Development of Information Society in the Republic of Azerbaijan" was mentioned among the measures for the development of national content. At the same time the "virtual society" is identified with "Internet society" in Azerbaijani-language sources and is interpreted as a new type of society created and operated in an electronic space.

The approaches of both terms in the literature show that both cyber space and virtual space are invisible world, also built using the computer network in terms of meaning. The concept of cyberspace is more common in English-speaking literature. However, concepts like "virtual environment" [19], "virtual world" [11] are also used and we can conclude that all of them have the same content with cyberspace. However, interpretations differ there. Some researchers note that, both cyberspace and virtual reality are connected with Internet and mass media: "Hypermedia can perform two functions: window function in objective world and subjective mirroring function. The first function covers virtual reality and the second-cyberspace. That is, if virtual reality reflects a well-perceived world, cyberspace defines precise conceptual basis of that world" [13]. "Virtual space" is regarded as a translation of either "cyberspace" category [16, p. 742], or it is claimed to be synonymous in Russian-language literature [15, p. 6]. In our opinion, both concepts "cyberspace" and "virtual space" are abstract and synonymous. Simply, depending on theoretical approach, some authors use the first term, while some authors use the second term. The concept of "cyberspace" is applied when it comes to the technical and management aspects, and the concept "virtual space" is used from social-humanitarian position. Considering that today there is no alternative network in the world, besides Internet, the concepts of virtual space and cyberspace should be

interpreted mainly on Internet.

Protection of human rights violated by cybercrimes. Today the violation of *personal privacy* and the use of personal information for illegal or unlawful purposes in cyberspace, which has become a major means of disseminating and transmitting information in the society are most often encountered. Therefore, the solution of this problem is one of the most important issues, world community facing.

The problem of protecting personal privacy in cyberspace was introduced in the United States in late 19th century. Thus, the article "The Right to Privacy" published in Harvard Law Review in 1890 by Samuel Warren (1852-1910) and Louis Brandeis (1856-1941) contains a lot of important points about personal life. The inviolability of private life and property were in fact recognized in common law since ancient times. Previously, the law provided resources more for preventing physical interference, and "vi et armis" (by force of arms) principle. However, gradual social, political and economic changes led human mind to be in the forefront and, consequently, the enlargement of rights, such as the inviolability of personal life and property. The right of personal inviolability already embraced a number of privileges and inviolability dominated not only material, but also intangible property..." [12, p. 193-220]

So the issue of inviolability of personal life did not arise from any body injury as in the past and intellect and information itself were regarded as a key element in the inviolability of privacy. Moreover, the determination of personal privacy, regardless of the physical, made the family relationships a part of the concept of privacy. Main goal of S.Warren and L.Brandeis in writing their article is analyzing legal regulation of issues of inviolability of privacy, offence, slander and other in such a new environment and its practical aspects. An interesting aspect of the article is that, the authors refer to many Roman law principles (postulates). For example, researchers who adhere to the principle of "damnum absque injuria" emphasize that even any act seeming formally legitimate and legal can be a threat to a person's private life. Authors showing as example the trial cases of Prince Albert v.Strange and Wilson, specifically point out Lord Cottenham's claim that "doctors who had been with George III during his illness were wrong in printing their diary notes" [4].

In their article, S.Warren and L.Brandeis also address the aspects of the right to privacy provided in the French legislation: the right to personal privacy does not prohibit the publication of any matter of state or public interest; the right to personal immunity does not prohibit communication (connection) in various forms; the right to personal immunity considered to have terminated since the permisson of legal fact's publication or since the time of its publication.

The problem of inviolability of private life was further analyzed in the article of William Lloyd Prosser (1898-1972) published in 1960. Thus, the author distinguishes four types of delicts, associated with the violation of inviolability of privacy: Irrational interference with person's life and location; Disclosure of personal information; Misrepresentation of identity information, i.e., dissemination of false information; Illegal acquisition or use of a person's name, surname and portrait for the purpose of earning income [14, p. 389].

Presently, the Republic of Azerbaijan has achieved a great success both in legal and practical terms in the field of personal data protection. Sufficient information was provided during the analysis of personal data on the legal framework. As far as practice is concerned, fast implementation of electronization processes across the country, the use of e-signatures, and other various cryptographic techniques reduced the number of interventions rather much with the right to privacy.

There exist many contradictions in the protection of *intellectual property rights* in the virtual space unlike right to privacy. The Chairman of the Copyright Agency of the Republic of Azerbaijan, K.S.Imanov, comments on the problem of intellectual property rights in cyberspace in two ways: The essence of the first argument is that the rights holders are not able to get overall benefit from the creation and distribution of the intellectual product. Because copying data, i.e., digital content in the digital period is cheaper and can make an exchange of large amounts of data over long distances. In this case, there is an unprecedented opportunity to replicate copies with perfect accuracy and to distribute them at instantaneous speed and at zero cost. The second conflict is that rights holders are often unable to bring charges against users of actual infringers because of their anonymity and widespread use of illegal content exchanges, and hence they charge the providers [1, p. 386].

Main problem with the protection of intellectual property rights in cyberspace is that the openness of Internet, i.e. easy access to information, increases the number of violation cases of

intellectual property rights. Even the authors call this kind of conflict the "Internet – Copyright" conflict [6, p. 197-213].

There are two approaches to the protection of intellectual property rights on Internet. According to the first approach, there is no need for intellectual property rights protection on Internet, which can hinder the development of the Internet. The recognition of a person"s non-property rights is sufficient in the best case. The second approach, on the contrary, considers the need for intellectual property rights protection on Internet, thus offering "collective rights management" way. This method is applied when individual protection of copyright and related rights is difficult. The objects of intellectual property are used in this case and legal owners are made payment in the prescribed manner [5, p. 238-252].

The activities of UNESCO on the protection of intellectual property rights in cyberspace should be emphasized. The organization launched a research project "Law and Society in Digital Age" in January 2006. Main objective of the project was to achieve a compromise between intellectual property owners and users. Primary activity started with a digital survey of intellectual property rights. According to the survey, a number of interesting facts were revealed. For example, 51% of surveyed legal owners believe that, main reason for the increase in piracy is not only legal gaps, but also low consumer awareness from legal aspect. Another example: 46% of the users and 44% of the proprietors spoke for the distribution of pirated products for non-commercial purposes and exposition to penalty by no means. On the contrary, they considered it necessary to impose more severe penalty on pirate production for commercial purposes [17, p. 9-12].

As cyberspace is space of information circulation, abuses of *freedom of expression* target human rights and freedoms. Thus, crimes committed through the realization of freedom of expression can be conditionally divided into two groups:

1. Criminals used cyberspace as a means of committing a crime, targeting various objects – public relations. For example, for crimes against peace and humanity include open calls for launching aggressive warfare (Article. 101 of the Criminal Code), crimes against constitutional basis and security of the state include incitement of national, racial, social or religious hate and hostility (Article. 283 of the Criminal Code). However, if mass media is used in both crimes a more severe penalty is imposed. The use of cybespace means the conduct of these crimes is an illegal realization of freedom of expression.

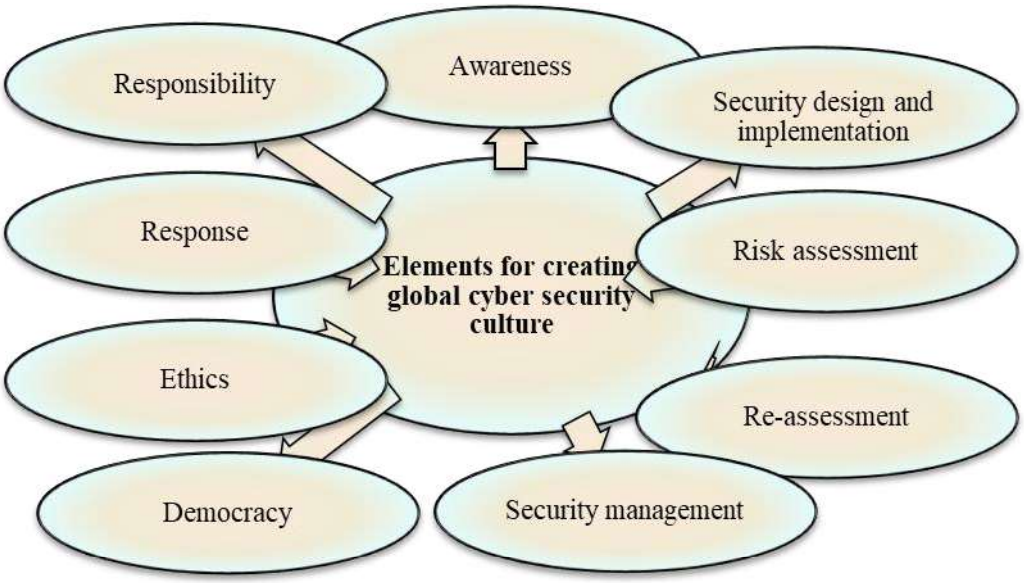
2. Crimes committed using cyberbspace in every case with conspiracy of honor and dignity. These crimes can be conducted in both verbal and written realization of freedom of thought and expression. For example, crimes including humiliation (Article. 148 of the Criminal Code of the Republic of Azerbaijan), slander (Article. 147 of the Criminal Code of the Republic of Azerbaijan) and defamation or humiliation of the honor and dignity of the head of the state - the President of the Republic of Azerbaijan (Article. 323 of the Criminal Code of the Republic of Azerbaijan).

The cases of violation of freedom of thought within cyberspace raised the issue of *hate speech* in recent years [10]. A number of international and local events were organized to implement freedom of thought and expression under normal conditions in recent years. Thus, the Council of Europe, which unites 47 countries launched *"No Hate Speech Movement"* campaign as a priority initiative in the Youth Sector for 2012-2017. This campaign defends and supports equality, dignity, human rights and diversity. The campaign aims at struggling against online expression of racist and discriminatory content speech by providing youth and youth organizations with the necessary skills to identify and resist against such human rights abuses.

Measures for the prevention of cybercrimes. The measures on the prevention of cybercrimes can be divided conditionally into *general and specific measures*. Specific measures may include the level of activity of people's self-defense from these threats. In this sense, the existence of a culture of information security is of particular importance. Technical knowledge and skills on information security, knowledge and skills about information threats for moral and psychological health of the person and ways to protect from and following legal and ethical norms upon the use of information resources make the basis of a person's *information security culture*.

Main source for building an information security culture is "Creating a Global Cyber Security Culture" approved by UN General Assembly Resolution. 57/239 dated December 20, 2002 and its appendix, "Elements for Building a Global Cyber Security Culture". Global cyber security culture requires to observe the following complement nine elements by all participants – government agencies, enterprises and other organizations, individual users that create, own,

manage, maintain and use information systems and networks:



According to the "Elements for Building a Global Cyber Security Culture", participants should be aware of the need for security of information systems and networks, and what they can do to enhance security, as well as their responsibility for the security of information systems and networks. Participants should take timely and joint measures to prevent, detect and respond to security incidents. They should make an exchange of information on the threats and void factors and apply procedures that ensure rapid and effective cooperation in preventing, detecting and responding such incidents. It might imply transboundary information sharing and cooperation. Security should be ensured in a democratic society to conform to accepted values, providing freedom of exchange of ideas and ideas, free flow of information, the confidentiality of information and communication, proper protection of personal information, lucidity and transparency [2].

"Elements for the Creation of Global Cyber Security Culture" defines a number of tasks not only for users, but also for specific states. It once again confirms that the culture of information security is a problem of the state interest. Mainly for this reason, increase of level of nationwide information security training and enlightement are reflected among strategic goals in the "Strategic Roadmap for the Development of Telecommunications and Information Technology in the Republic of Azerbaijan", approved by the Decree of the President of the Republic of Azerbaijan dated December 6, 2016. The enhancement of information security culture in national strategies is implied to be one of the expected outcomes of such education.

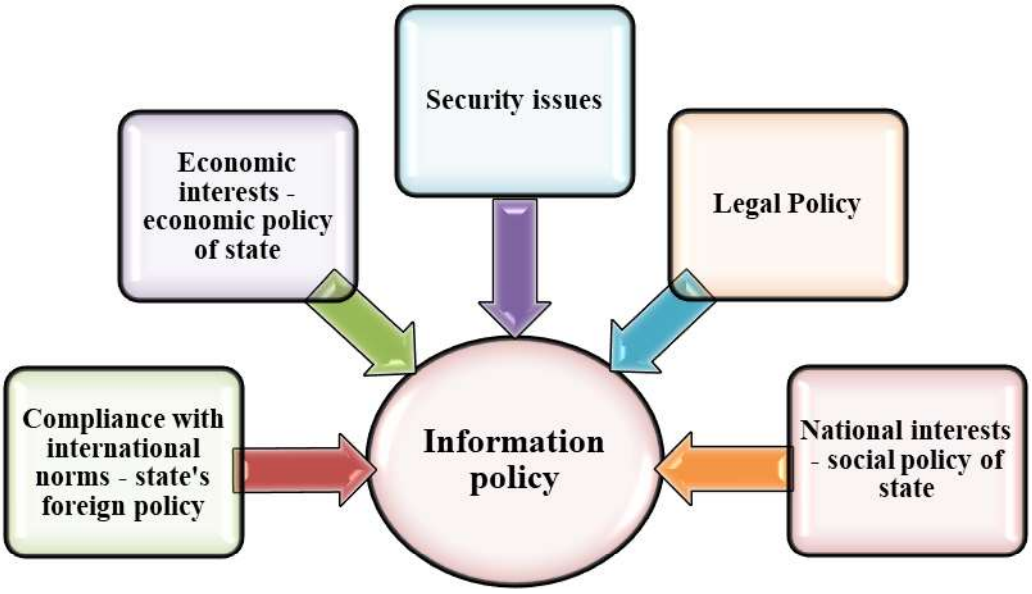
General measures on the prevention of cybercrimes are carried out by the state. First of all, determination of liability for various violations and the imposition of sanctions should be noted. Traditionally, there distinguished four types of liability: criminal, administrative, civil, and disciplinary, respective of the nature of the legal breaches. However, today such concepts as international legal responsibility, constitutional and legal responsibility are also encountered.

Another common action plan should include information security as one of the areas of *national information policy*. The Information for All Programme (IFAP) identifies five priorities in the National Information Society Policy (MICS): Information for development; Information culture; Maintaining information; Information Ethics; Accessibility of information [9, p. 9-10].

Apparently, national information policy includes a system of measures and rules aimed at ensuring access to information for society as a whole. Information policy is divided into two parts depending on the nature of the issues solved: *information strategy and information tactics.* Information strategy is a model of planned action aimed at solving large-scale information problems, which is directed to the successful completion of information processes and the unrestricted provision of information rights and freedoms. Information tactics are formed on the basis of information strategy and includes specific measures to achieve the goals and objectives. It means that, information strategy answers the questions "what" and "why", while information tactic answers the question "how". Information tactics are characterized by

agility unlike strategy. For example, a number of state programs – "State Program on Development of Communication and Information Technology for 2005-2008 In the Republic of Azerbaijan (Electronic Azerbaijan) ", etc. were accepted with the purpose of implementation of "National Strategy on Information and Communication Technologies for the Development of the Republic of Azerbaijan (2003-2012)", approved by the Decree No. 1146 of the President of the Republic of Azerbaijan dated February 17, 2003 and these programs reflect the state's information tactics.

Implementation of the national information policy is impossible without considering other aspects of the state. Thus, it would not be logical to talk about the processes of informatization and electronicization and the availability of information in an economically ineffective environment. On the other hand, an information policy that does not take into account national interests cannot be successfully fulfilled. Also, an information policy that does not comply with international standards and has no legal basis will ultimately lead to a conflict of interests. On the other hand, it is impossible to achieve normal implementation of information policy under conditions which national security is not protected. It is no coincidence that law of the Republic of Azerbaijan "On National Security" dated June 29, 2004, provides national security in the field of information as a separate field (Article 15.1). Therefore, the state's information policy is implemented in a mutually interrelated manner with economic and legal measures, taking into account international and national interests and providing national security.



The scheme clearly shows that, national information policy refers to a complex system of measures implemented by state authorities. The question arises: can concentration of national information policy only on state authorities mean human rights and freedoms restriction? – No. In fact, state always existed as a governing body for the commitments such as provision of rights and freedoms, prevention of violations, etc. It is impossible to achieve the goals without the role of the state at a time when the idea of a legal state is so widespread. Supervision over the activities of state bodies is definitely an important factor. Mainly for this reason, "mutual responsibility – the responsibility of the person before the state and the state before the person" is guided as one of the basic principles of the legal state. At the same time, proposing the ideas of open government, public control, civil society and other ideas have an important impact on the implementation of the national information policy of the state.

Conclusions. The globalization of all sectors of society and the formation of cyberspace open opportunities for offenders along with law-abiding citizens to conduct breaches in easy ways. Struggle against cybercrimes, one of the most topical problems of the present time, is being implemented on a global scale. Since the search for a criminal in an unknown location is extremely difficult, cybercrimes should be treated with "sensitivity" both at national and international levels.

We can even say that cybercrime can have more serious consequences than tradi-

tional crime. The principle of cooperation to prevent cyberbullying should be guided in this regard. If it is implemented in two directions, more efficient results can be achieved: cooperation of states at international level and cooperation between citizens and state bodies at national level.

References

1. Aliyev A.I., Rzayeva G.A., Ibrahimova A.N., Maharramov B.A., Mammadrzali S.S. Information law. Textbook. Baku: Nurlar, 2019, 448 p.
2. Creation of a global culture of cybersecurity: resolution / United Nations General Assembly (UNGA) Resolution 57/239, 31 January 2003. URL : https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unga-creation-global-culture-cybersecurity.
3. Darrel C. Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review*, 1998, Volume 4, Issue 1, p. 69-103.
4. Dorothy J. Glancy. The invention of the right to privacy. *Arizona Law Review*, 1979, Volume 21 (1). URL : http://law.scu.edu/wp-content/uploads/Privacy.pdf.
5. Dutfield G. Global intellectual property law: commentary and materials / Graham Dutfield [and others]. Northampton, MA: Edward Elgar Pub., 2005, pp. 238-252.
6. Fiordalisi E. The Tangled Web: Cross-Border Conflicts of Copyright Law in the Age of Internet Sharing. *Loyola University Chicago International Law Review*, 2015, Vol. 12, İssue 2, pp. 197-213.
7. Gibson W. Burning chrome. Canada, 1982. URL : http://project.cyberpunk.ru/lib/burning_chrome/
8. Gibson W. Neuromancer. First edition, 1984, 271 p.
9. National information society policy: A template. Developed by The Information For All Programme of UNESCO. Paris November 2009, 143 p.
10. Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech". / Adopted on 30 October 1997 by Committee of Ministers of Council of Europe. URL : https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-97-20-of-the-committee-of-ministers-to-member-states-on-hate-speech-?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/.
11. Richard R. Bartle. Designing Virtual Worlds. New Riders, 2003, 741 p.
12. Samuel D. Warren, Louis D. Brandeis. The Right to Privacy. Harvard Law Review, 1890, Vol. 4, No. 5, p. 193-220.
13. W.Lambert Gardiner. Virtual Reality/Cyberspace: Challenges to Communication Studies. *Canadian Journal of Communication*, 1993, Vol 18 (3). URL : http://www.cjc-online.ca/index.php/journal/article/view/762/668
14. William L.Prosser. Privacy. *California Law Review*, 1960, Volume 48 (3), p. 383-423.
15. Рассолов И.М. Право и Интернет: Теоретические проблемы. Москва: Норма, 2009, 383 с.
16. Телешина Н.Н. Виртуальная пространства как новая юридическая конструкция: к постановке проблемы. *Юридическая техника*, 2013, №7 (Ч.2), с. 740-747.
17. Туликов А. Интеллектуальная собственность в киберпространстве: правообладатели и общество готовы к диалогу. *Интеллектуальная собственность в киберпространстве: Сборник аналитических материалов проекта "Право и общество в цифровую эпоху"*. М. : МОО ВПП ЮНЕСКО "Информация для всех". Составитель: Евгений Альтовский, 2006, с. 9-12.
18. URL : http://virtualaz.org/.
19. URL : http://www.dictionary.com/browse/virtual-environment.
20. URL : http://www.virtualkarabakh.az/index.php?lang=3.
21. URL : https://www.eff.org/cyberspace-independence.

Received to editorial office 14.03.2020

SUMMARY

Changing and developing world outlook in modern society also has an impact on illegal behavior. As traditional methods do not meet the requirements of the time, ICTs are increasingly being used as a new method and tool for violating human rights and committing different offences. This also requires strengthening the fight against cybercrimes. In the article were put forward suggestions and recommendations for the development of human rights protection mechanisms that have been violated by cybercrimes in the global information society.

Keywords: *global information society, cyberspace, cybercrime, freedom of expression, right to personal privacy, intellectual property rights, information policy.*