UDC: 004.056: 341 (045)

Shyrokova-murarash o.g., Associate Professor,
Akchurin Y.R., Senior Lecturer
(National Aviation University, Ukraine)

International legal aspect of international information security

Abstract. The problem of international legal bias of cybercrime and cyberterrorism as a result of the negative impact of information technology on society.

Annotation. On the problem of international legal prevention of cybercrime and cyberterrorism as a result of the negative impact of information technology on society.

Summary. As to the problem of international law prevention of cyber crime and cyber terrorism as a result of the negative impact of information technologies on the society.

The modern world cannot be imagined without informational and communicative technologies (hereinafter - ICT), which transformed not only the principles and forms of collecting, processing and transmission of information; they began to exert a powerful influence on the cultural, economic, political, military-strategic aspects of public life. At the same time, the development of ICT has caused not only the transition of national infrastructures to a fundamentally new level of development and functioning, but also created fundamentally new threats to national and international security systems and created a whole range of negative geopolitical consequences. These threats are primarily related to the possibility of using ICT for purposes incompatible with maintaining international stability and security, adherence to the principles of non-use of force, non-interference in the internal affairs of states, respect for human rights and freedoms.

The aim of the theses is to highlight the danger of uncontrolled use of information and communication technologies and to determine the ways of normative regulation of issues of international information security.

International law only starts the way of its regulation. On May 10, 1999, the UN Secretary General made a report (A/54/213), which recognized the existence of a problem in the field of international information security (hereinafter - IIB).

Resolution No. 53/70 initiated a discussion on the need for a new international legal regime to regulate the area of information space, ICT and its methods of use [4]. In 1999, an international seminar on international information security was held in Geneva. Representatives of more than 50 countries took part in this seminar. The result was the confirmation of the relevance of the problem of information security and the current state of this issue in the international plan. At the 54th session of the General Assembly of the United Nations, a draft resolution entitled "Achievements in the field of information and telecommunications in the context of international security" was proposed. An important point was that it was

for the first time expressed concern about the potential use of ICT "with goals that are incompatible with the objectives of ensuring international stability and security", which could have a negative impact on the security of states in both civilian and military spheres. Considering that it is necessary to prevent "the illegal use or use of information resources or technologies for criminal or terrorist purposes," the General Assembly raised the question of "the feasibility of developing international principles aimed at strengthening the security of global information and telecommunication systems and contributing to the fight against information terrorism and crime" [5]. The Russian side prepared a draft Principles of International Information Security, which was published in the document of the 55th General Assembly of the UN No. A / 55/140. It contains the necessary conceptual framework and sets out the main definitions: international information security, threats to information security, information weapons, information warfare, international information terrorism and crime. The five basic principles of international information security determine the role and rights, obligations and responsibilities of States in the information space.

The resolution adopted by consensus on 29 November 2001 (document No. A / RES / 56/19) endorsed the idea of establishing in 2004 a Special Group of Governmental Experts from the Member States of the United Nations (UNESCO) for a comprehensive study of the IIB problem [8]. The mandate of the Group is to consider existing and potential threats in the field of information security and possible joint measures for their elimination, as well as study of international concepts that would be aimed at strengthening the security of global information and telecommunication systems. The results of the work of the Group in accordance with the resolution will be the report of the UN Secretary-General to the General Assembly in 2005 on the results of this study.

In the next period, implementation of the decision of the international community on the need for a broad practical study of IIB issues, resolutions are adopted that develop the provisions of the previous resolutions and confirm the inadmissibility of the use of information and telecommunication technologies and tools to negatively affect the infrastructure of States. On January 23, 2002 the 56th UN GA adopts a resolution on the topic "Fighting against the criminal use of information technology", which referred to the need for international cooperation, as well as the interaction between States and the private sector in combating the criminal use of ICT, and the need to facilitate the provision of ICT to countries, that are developing since incompatibility of different states' development in the context of the access to ICT and their use may reduce the effectiveness of the fight against crime in this area [6]. In 2002, at the Pan-European Conference in Bucharest, a declaration was adopted that consolidated the principle of strengthening trust and security in the use of ICT. It envisages the development of a "global culture of cyber security" that should be provided through preventive measures and maintained by the entire community, while maintaining the freedom to transmit information. The countries agreed that "it is necessary to" prevent the use of information resources or technologies for criminal or terrorist purposes "and to strengthen international cooperation in this area [8].

The Tokyo Declaration (January 13-15, 2003), which was adopted by representatives of 47 countries, 22 international and 116 non-governmental organizations, as well as representatives from 54 private companies, highlighted the "priority areas" of ICT activities. An important part among them is the issue of security of information technologies and facilities. While recognizing the principle of just, equitable and adequate access to ICT for all countries, the parties consider it necessary to endanger the potential military use of ICT. For the first time, the view was expressed that the effective provision of information security can be achieved not only technologically, but also requires efforts to regulate legal issues and develop appropriate national policies [2].

Finally, according to UN General Assembly resolutions 56/183 of 21 December 2001 and 57/238 of 20 December 2002 took place in Geneva. On December 10-12, 2003 the first stage of the World Summit on the Information Society took place (the second one was scheduled for November 16-18, 2005 in Tunisia). The meeting turned out to be the first international forum in which the discussion of issues related to the global processes of informatization was violated at the highest political level and took place on a broad geopolitical scale in dialogue with representatives of business circles and civil society. The summit was attended by over 11,000 people from 176 countries, including representatives of international organizations. During the meeting, the issue of information security was at the center of international attention.

The outcome of the first phase of the meeting was the adoption of two documents - the Declaration of Principles and the Plan of Action. They cover various aspects of the formation of the global information society and the basic directions of intergovernmental cooperation in this area, including the creation and development of information and communication infrastructure, ICT security, access to information, ICT infrastructure and services [8]. The Declaration of Principles (section "Strengthening trust and security in the use of ICT") indicates that building a solid foundation for trust, including information security and network security, is a prerequisite for the emergence of an information society.

Important aspects of the fight against information crime were recorded in the Resolution of the 58th UN General Assembly of January 30, 2004 entitled "Creating a Global Culture of Cybersecurity and Protecting Major Information Structures." The most significant of these is the formulation of a list of elements to protect the most important information infrastructures. That is, those protective mechanisms, both international and national, were indicated, which are the basic elements for building a global system to counter attempts to use and use ICT for purposes incompatible with the basic principles of international law and the security of states, societies and individuals.

Conclusions

As a result, we note that the latency of developing information warfare tools, the role of ICT in dual-use technologies, and the combination of these technologies with traditional means of engagement while virtually uncontrolled creation, use and

weak regulation of cyberspace can lead to catastrophic consequences for the existence of human civilization. This can be prevented only by international cooperation of all states in the field of information security, which, on the basis of balanced international legal acts considering the specificity of national legislation and the existence of political will, shall ensure the establishment of an effective system of international information security.

References

1. Inozemtsev VL, Kuznetsova E.S. Atlas 2010. Le monde diplomatique / VL Foreigners - M.: Center for the Study of Post-Industrial Society, 2010. - 224 pp.

2. Mode of access: //www.portalus.ru/modules/internationallaw/rus_readme.php?

3. A.V. Krutskyh, I.L. Safonova International cooperation in the field of information security. - Access mode: //www.ict.edu.ruft002472intcoop.pdf).pdf

4. Combating the criminal use of information technologies: Resolution of the UN General Assembly No. 53/70 dated 04.01.99. - C. 1-2. - Access mode: //www.un.org/russian/documen/gadocs/53sess/53reslis.htm

5. Achievements in the field of informatization and telecommunications in the context of international security: UN General Assembly resolution 54/49 of September 23, 1999 - C. 1-2. - Access mode: //www.un.org/russian/documen/gadocs/54sess/54reslis.htm

6. Developments in the field of informatization and telecommunications in the context of international security: UN General Assembly resolution No. 56/121 dated January 23, 2002 - C. 1-2. - Access mode: //www.un.org/russian/documen/gadocs/56sess/56reslis.htm

7. Creation of a Global Cybersecurity Culture: United Nations General Assembly Resolution No. 57/239 of January 31, 2003 - C. 1-3. - Access mode: //www.un.org/russian/documen/gadocs/57sess/57reslis.htm

8. International cooperation in the field of information security (background information). - Access mode: //www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256e320029b1ef?OpenDocument