leaders in the European Council. Examples include recommendations to combat ineffective public procurement practices, strengthen rules to prevent conflicts of interest, review statutes of limitations for corruption offenses, or resort to informal payments in the healthcare sector.

1. The official website of Transparency International [Electronic Resource]. - Access mode: https://www.transparency.org/. - Date of acces: 08/04/2019.
2. Official website of the European Commission against Corruption [Electronic resource]. – Access mode: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/corruption_en. - Date of access: 08/04/2019.

UN LEGAL SOURCES IN THE FIELD OF REGULATION OF ONLINE SPACE AT THE PRESENT STAGE

Darya Mazurtsova
VSU named after P.M. Masherov, Vitebsk, Belarus

Providing a stable and secure online environment is no longer an exclusive problem of the technology and software sector. Recently, more and more attention has been paid to the regulation of the Internet sphere, which is directly related to the rapid globalization, the widespread integration of states, the projection of the main spheres of society onto the online space, the emergence of legal gaps in the field of ensuring human rights, new threats to state security, expanding the scope of attackers, the difficulty of accurately identifying the location of hackers, and, as a consequence of this, the need for criminal law cooperation of present states.

The purpose of this study is to analyze the legal activities of UN bodies in the field of cyberspace regulation in connection with the rapidly arising legal conflicts in this area.

Material and methods. The main materials of the study are the Resolution “Creation of a global culture of cybersecurity” dated 01.01.2003 No. 57/239, Draft Convention on International Information Security, etc. The formal legal method as well as analysis and generalization were used in the study.

Findings and their discussion. The obvious insufficiency and inefficiency of unilateral actions of states in ensuring stable cybersecurity places a serious responsibility on the international community for the formation of unified integrated systems countering online threats. The leading organization in the field of facilitating the creation of a uniform approach to the pressing problems of our time is the UN, which has repeatedly recognized the urgent need for a solution to the key problems of insufficient Internet regulation.

Already in 2003, the UN General Assembly adopted the Resolution “Creation of a global culture of cybersecurity”, which was one of the first to draw attention to the very concept of “cyber security” and developed a number of inevitable components of its achievement. The formation of an online community cannot be denied, its influence on all spheres of life in modern society is becoming stronger every year, and therefore the Resolution proposes to set the goal of achieving the state of the greatest protection of a person and society from cyber threats. There is the emphasize on the fact that cybersecurity cannot be achieved individually, it is not a problem of one state and its government, widespread cooperation should be provided in this area. The General Assembly has developed nine complementary elements for achieving cybersecurity: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, reassessment. In the disclosure of the above elements the Resolution sees direct instructions for the interaction of states and other participants in online relations [1].

It is worth noting that the UN, as a member of the online space, has repeatedly become a victim of insufficient cyber security. In 2013, the Report of the UN Secretary General was submitted, an operational action plan was developed to eliminate comments in this area based on the results of the work of the Board of Auditors on the vulnerability of information systems of the UN Secretariat. The problems noted in the Report are ubiquitous. First of all, the Report paid special attention to technical equipment and ensuring systematic monitoring by invited experts of the relevant specialization, strengthening preventive control measures, checking all software packages, timely detection of unauthorized access attempts, installing degree assessment systems security. Directly confronted with the problem of cyber security, the UN is actively proposing the most effective ways to respond to cyber-attacks [2].

In 2015, the United Nations Economic and Social Commission for Western Asia presented Political Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region. The study provides an analytical overview of the current situation with cybercrime and cybersecurity at the regional and international levels, highlights measures of strengthening and harmonizing efforts to combat cyber-crime and provides a legislative framework for enhancing cybersecurity and confidence in information and communication technology and cyberspace. The document emphasizes the need to reinforce the regulatory and procedural framework for combating cyber threats and raising awareness of individuals and institutions about such risks and their impact on work and personal life [3].

The next step towards achieving cybersecurity was the development of a Draft Convention on International Information Security. The purpose of the Convention is to counteract the use of information technology for violating international peace and security. The draft document provides the obligation of states to cooperate with each other during the formation of an international information security system, guided by the principles of the indivisibility of security and responsibility for their own information space, states should strive to reduce the “digital division” in order to reduce the overall level of threats to information space, etc. The main emphasis is placed directly on information security, and, unfortunately, no special attention is paid to cybersecurity that has its own characteristics, which complicates the complete regulation of online environment [4].

In addition to the direct regulation of cyberspace with the help of special regulatory instruments, a group of government experts on cybersecurity operates within the UN. A number of divisions, whose field of activity intersects with the online space, are engaged in some issues of cybersecurity, such platforms are ITU, UNIDIR, CTITF Working Group, UNODC, UNICRI [5].

Conclusion. Thus, the UN competent authorities are trying to respond quickly to emerging legal gaps in the field of cyber law, but the proposed solutions are often targeted and local. Unfortunately, at the moment there is no fundamental international act that would identify the problems and lay down the principles of ensuring cybersecurity. Perhaps the UN should develop such a document in order to prevent the emergence of further legal conflicts in the field of an operational response to cyber threats both at the international and local levels. There is a need to consolidate at the international level a list of issues that are directly related to the basis of the state of cybersecurity, the definition and classification of types and levels of cyber aggression. The progressive step could be the formation of specialized bodies of an international level competent in countering cyber threats, including outside the territorial jurisdiction of states in exceptional cases.

1. Resolution adopted by the General Assembly "Creation of a global culture of cybersecurity" [Electronic resource]. – Available at: https://undocs.org/ru/A/RES/57/239. – Accessed: 28.10.2019.
2. Report of the Secretary-General Progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat" [Electronic resource]. – Available at: https://undocs.org/ru/A/68/552. – Accessed: 29.10.2019.
3. Recommendation on Cyber safety and Combating Cybercrime in the Arab Region: Summary [Electronic resource]. – Available at: https://www.unescwa.org/sites/www.unescwa.org/files/uploads/policy-recommendations-cybersafety-arab-region-summary-english.pdf. – Accessed: 30.10.2019.
4. Draft Convention on International Information Security [Electronic resource]. – Available at: https://www.pircenter.org/kosdata/page_ doc/ p2728_1.pdf. – Accessed: 31.10.2019.
5. Tim Mauer Cyber norm emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-security [Electronic resource]. – Available at: https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf. – Accessed: 01.11.2019.