UDK 341.1.8

Paziuk Andrii,
Doctor of Juridical Science, Associate Professor of the Department of International Law, Institute of International Relations, Kyiv Taras Shevchenko National University
prof.cyberlaw@gmail.com
ORCID 0000-0002-1622-1671
Mitsik Vsevolod,
Doctor of Juridical Science, Professor, Head of the Department of International Law, Institute of International Relations, Kyiv Taras Shevchenko National University
mitsik56@gmail.com
ORCID 0000-0002-7008-1577

GLOBAL CYBERSECURITY CULTURE IN THE INTERNATIONAL DISCOURSE: VALUES AND PRINCIPLES

The purpose of the article is to analyse the development trends of the global culture of cybersecurity in contemporary international discourse devoted to outlining and framing the institutional and legal modalities for responsible behaviour of states and other actors in cyberspace. **Methodology.** The research methodology integrates dialectic, analytical and comparative methods. **The scientific novelty** lies in the revealing of the differences in political priorities, despite the formal consistency of the values, at the current stage of international discourse around the rules of responsible behaviour of a State in cyberspace emerged from the analysis of the results of the discussions of the First Committee of the UN General Assembly at its 73rd session (October 2018) entitled ‘Developments in the field of information and telecommunications in the context of international security’. **Conclusions.** The international discourse around the values and principles of the global cybersecurity culture is at an early stage and is essential for the formation of a coordinated position of international political actors regarding norms of responsible behaviour in cyberspace. In such way, by identifying the influencing factors and the ruling forces on behalf of the political actors, it is possible to understand the trends and predict its perspectives both from the point of view of institutionalization in the contemporary international order and legal framework that embody and protect human values as a core component of global culture in cyberspace.

Keywords: cybersecurity; cybersecurity culture; values and principles, responsible behaviour in cyberspace; human rights; international law and order.

***Пазюк Андрій Валерійович**, доктор юридичних наук, доцент кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка; **Мицик Всеволод Всеволодович**, доктор юридичних наук, професор, завідувач кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка*

Глобальна культура кібербезпеки в міжнародному дискурсі: цінності та принципи

Мета статті полягає в аналізі тенденцій розвитку концепції глобальної культури кібербезпеки в сучасному міжнародному дискурсі, що проявляється у пошуку організаційно-правових моделей для розробки і прийняття правил відповідальної поведінки держав та інших акторів в кібер-просторі. **Методологія** дослідження полягає у застосуванні комплексного підходу з використанням діалектичного, аналітичного і порівняльного методів. **Наукова новизна** отриманих результатів полягає у виявленні розбіжностей у політичних пріоритетах попри формальну узгодженість щодо ціннісних чинників на сучасному етапі міжнародного дискурсу навколо правил поведінки в кіберпросторі, що випливає з аналізу результатів роботи Першого Комітету Генеральної Асамблеї ООН на 73-й сесії (жовтень 2018 р.) щодо розгляду питання про досягнення в сфері інформаційно-комунікаційних технологій в контексті міжнародної безпеки. **Висновки.** Міжнародний дискурс навколо цінностей і принципів розбудови глобальної культури кібербезпеки знаходиться на початковій стадії і є важливим для формування узгодженої позиції міжнародних політичних акторів щодо норм відповідальної поведінки в кібер-просторі. Виявлення чинників впливу і рушіїв розвитку цього напрямку в міжнародному співробітництві дозволяє усвідомити тенденції і спрогнозувати подальші його перспективи як з точки зору інституціоналізації в сучасній системі міжнародного правопорядку, так і наповнення нормативними приписами, що втілюють і захищають загальнолюдські цінності як складову глобальної культури в кіберпросторі. Створення глобальної культури кібербезпеки є можливим за умови досягнення консенсусу щодо основоположних цінностей і пріоритетів, а також їх ствердження шляхом закріплення в універсальному міжнародно-правовому договорі.

Ключові слова: кібербезпека; культура кібербезпеки; цінності і принципи; відповідальна поведінка в кіберпросторі; права людини; міжнародний правопорядок.

***Пазюк Андрей Валерьевич**, доктор юридических наук, доцент кафедры международного права Института международных отношений Киевского национального университета имени Тараса Шевченко; **Мицик Всеволод Всеволодович,** доктор юридических наук, профессор, заведующий кафедрой международного права Института международных отношений Киевского национального университета имени Тараса Шевченко*

Глобальная культура кибербезопасности в международном дискурсе: ценности и принципы

Цель статьи заключается в анализе тенденций развития концепции глобальной культуры кибербезопасности в современном международном дискурсе, что проявляется в поиске организационно-правовых моделей для разработки и принятия правил ответственного поведения государств и других актеров в киберпространстве. **Методология** исследования заключается в применении комплексного подхода с использованием диалектического, аналитического и сравнительного методов. **Научная новизна** полученных результатов заключается в выявлении расхождений в политических приоритетах несмотря на формальную согласованность в отношении ценностных факторов на современном этапе международного дискурса вокруг правил поведения в киберпространстве, что следует из анализа результатов работы Первого комитета Генеральной Ассамблеи ООН на 73-й сессии (октябрь 2018 г.) по рассмотрению вопроса о достижениях в сфере информационно-коммуникационных технологий в контексте международной безопасности. **Выводы.** Международный дискурс вокруг ценностей и принципов развития глобальной культуры кибербезопасности находится на начальной стадии и является важным для формирования согласованной позиции международных политических актеров относительно норм ответственного поведения в киберпространстве. Выявление факторов влияния и двигателей развития этого направления в международном сотрудничестве позволяет осознать тенденции и спрогнозировать дальнейшие его перспективы как с точки зрения институционализации в современной системе международного правопорядка, так и наполнения нормативными предписаниями, воплощающими и защищающими общечеловеческие ценности как составляющую глобальной культуры в киберпространстве. Создание глобальной культуры кибербезопасности возможно при условии достижения консенсуса в отношении основополагающий ценностей и приоритетов, а также их утверждения путем закрепления в универсальном международно-правовом договоре.

Ключевые слова: кибербезопасность; культура кибербезопасности; ценности и принципы, ответственное поведение в киберпространстве; права человека; международный правопорядок.

Research rationale. In 2003, the United Nations General Assembly adopted the Resolution «Creation of a global culture of cybersecurity». It invited states to develop throughout their societies a culture of cybersecurity in the application and use of information technologies by all «participants», such as «Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks» [16]. The word «global» regarding the culture of cybersecurity reflects the universality of the approach and broad coverage of the organisational, local and international cybersecurity levels.

In the later documents, endorsed at international fora, the «cybersecurity culture» concept covers the range of the topics as a feature of individual users' security, as an element of corporate culture and security management or as the ethical concerns with regard intrusive methods of information security audit. The audience of such discussions includes IT-companies' managers, technical and engineering personnel, and cybersecurity experts [2].

However, cybersecurity culture at international level, in the relationships between states and intergovernmental organisations is ambiguous, geopolitically vulnerable and extremely important for maintaining international security. It is well illustrated by the work of the First Committee of the General Assembly of the United Nations at the 73rd session, when two drafts of resolution on the same item initiated by two geopolitical opponents - the United States and the Russian Federation. Both resolutions define the need to develop standards of responsible behaviour of states in cyberspace, but with different goals and mechanisms of implementation.

There is a need to research the reasons behind such tendencies in international politics and to predict scenarios of international discourse concerning the global culture of cybersecurity, which also determines the relevance of this article. The practical outcomes of this research can be found in the improved understanding of the problem, which will allow formulating scientifically grounded position of the foreign policy of state, the business community and civil society as «participants» of the global culture of cybersecurity.

The analysis of existing researches and publications on the subject indicates that, for the most part, the culture of cybersecurity is considered as an attribute of corporate culture [2; 3, 14-18; 11], or the philosophical category of ethics adapted to the concept of cybersecurity, including the right to privacy and surveillance, intellectual property and piracy, codes of conduct, and so on.

Among the research works that in some way relate to the global (intergovernmental) culture of cybersecurity there are those that are devoted to geopolitics and law [6, 35-54], cyber-norms, both existing and emerging in various spheres of international co-operation [4, 425-479; 10; 13]. At the same time, priorities and value orientations for defining the normative content of the rights and responsibilities of key political actors in cyberspace and the formation of a global culture of cybersecurity remain inadequately explored.

The purpose of the study is to analyse the trends in contemporary international discourse around the global culture of cybersecurity, foundation of intergovernmental framework for the development and endorsement of the rules of responsible behaviour of states and other actors in cyberspace. The interstate and multistakeholder, involving business and civil society, initiatives on defining the normative content of the rights and responsibilities of major political actors in the international arena seem to have a non-systematic and controversial nature that has so far prevented consensus and universal acceptance at the universal international level. The authors aimed to identify the central contradictions in the correlation of political priorities and value orientations. It predetermines such trends and predicts the most probable scenarios for the regulation of cybersecurity issues at the global level. It also influences foreign policy of a state, the support by business community and civil society as participants of international discourse.

The presenting of the primary material. There is annexe to the UN General Assembly Resolution 57/239 «The creation of a global culture of cybersecurity» with nine «Elements for creating a global culture of cybersecurity» that can be considered as a basis for developing relevant principles, in particular: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. Some of them are repeated at international initiatives aiming to develop normative framework for meaningful content of the cyber-security culture concept. At the main cybersecurity session of the Internet Governance Forum in 2015, the speaker started with such words: «As the cyberspace expands itself, adding more and more networks, we also have an increase in risks inherent to the use of this space. Consequently, an increase in the improvement of Cybersecurity is required in order to protect the space and contribute to its use with freedom and ethics. At the same time, Cybersecurity shows very clearly that the success of this process essentially depends on intense collaborative action. It requires building and maintaining trust relationships among all involved parties. And like in any other trust relationships, we need initiatives to bring people closer, mutual knowledge and convincing demonstrations of respect for people's values and rights»[7].

French President E. Macron announced Paris Call «For Trust and Security in the Cyberspace» in November 2018, joined by sixty states and several hundred companies and civil society organisations. The document indicates the aspirations of the participants «to assist one another and implement cooperative measures, notably in order to:

prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;

prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;

strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;

prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;

develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;

strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain;

support efforts to strengthen advanced cyber hygiene for all actors;

take steps to prevent non-State actors, including the private sector, from hacking-back, for their purposes or those of other non-state actors;

promote the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures in cyberspace» [8].

As we can see from this and other mentioned documents, the concept of a cybersecurity culture can cover different elements and addresses in different contexts, topics including national security, information and critical infrastructure protection, the safe use of information and communication technologies. The priorities determining the importance of this or that component of cybersecurity culture are established and maintained by international actors that offer or support one or another initiative in the international discourse. Therefore, meaningful (contextual) analysis of documents on keywords that embodies social values will reveal the priority of values for the relevant actors.

The link between values and political priorities for the formation of the concept of a cyber-security culture can also address the development of draft documents in the framework of multilateral processes involving the representatives of states, business and civil society actors. That can be illustrated by the research paper presented by «An Internet Free and Secure» working group, which was established via multistakeholder framework of the Freedom Online Coalition. The working group has set itself the goal of developing its definition for the concept of cybersecurity, which would be consistent with such values as individual freedom and security. As the participants note, «working group believes very strongly that individual security is a core purpose of cybersecurity and a secure Internet is central to human rights protection in the digital context… Cybersecurity and human rights are complementary, mutually reinforcing and interdependent. Both need to be pursued together to promote freedom and security effectively. Recognising that individual security is at the core of cybersecurity means that protection for human rights should be at the centre of cybersecurity policy development» [1]. The elaborated definition is universal: «Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure to enhance the security of persons both online and offline» [1].

This definition reaffirms that security and freedom (as well as cybersecurity and human rights) are deeply interconnected and synergistic, mutually reinforcing each other. The proposed understanding of the culture of cybersecurity is worthy of universal recognition, it explores the categories of «security» and «freedom» as interdependent. Therefore, the use of the keywords «human rights» for the contextual search in the documents of international discourse around the creation of a global culture of cybersecurity will make it possible to prioritise human rights among other values for process participants.

One of the processes analysed in this study is the «global consultation» of the High-Level Group of the United Nations Secretary-General for Digital Co-operation, which took place from October 8, 2018, to January 31, 2019. Among the issues, that the participants had to answer there was: «What values and principles should underpin cooperation in the digital realm» [14].

Based on the contextual analysis of 97 (ninety seven) posts, we found that human rights have received high (above 50%) the level of priority among the values for the participants of the consultations: for representatives of the media industry - 50%; Academic community - 55%; IT business - 56%; civil society and intergovernmental organizations - by 67%; for governments - 75% [15]. These data indicate the different level of priority of such a value as human rights in the international discourse for various political stakeholders - participants in multilateral negotiation processes around the digital agenda for the development of humankind.

However, the differences in the values and principles that should be the basis of the global culture of cybersecurity are not the only one ground for the existent debate. Due to differences in approaches and the inability to reach a compromise, the work of the UN Group of Governmental Experts (GGE) on the developments in the field of information and technologies in the context of international security (2016-2017) was unsuccessful. In addition, representatives of some states tried to question and to revise the previous achievements of the GGE, which were most active in 2013 and 2015 [17; 18]. Among the most significant achievements is recognition of the fact that the UN Charter is applicable in the cyberspace, as well as a dozen of norms-principles that enhance stability and security and lay the foundations for a global culture of cybersecurity.

In November 2018, the First Committee of the UN General Assembly discussed the agenda item titled the «Developments in the field of information and telecommunications in the context of international security». The positions of the participants regarding the topic showed the existent geopolitical struggle for the influence in the international fora. The draft of the resolution initiated by the United States and supported by Western countries (Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Malawi, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, United Kingdom of Great Britain and Northern Ireland and United States of America) proclaims the values and commitment of democratic states to ensure open, interoperable, a reliable and secure information and communication technology environment consistent with the need to preserve the free flow of information [19].

Instead, a draft resolution submitted by the Russian Federation and supported by a number of other states (Algeria, Angola, Azerbaijan, Belarus, Bolivia, Burundi, Cambodia, China, Cuba, Democratic People's Republic of Korea, Democratic Republic of the Congo, Eritrea, Iran, Kazakhstan, Lao People's Democratic Republic, Madagascar, Malawi, Namibia, Nepal, Nicaragua, Pakistan, Samoa, Sierra Leone, Suriname, Syrian Arab Republic, Tajikistan, Turkmenistan, Uzbekistan, Venezuela and Zimbabwe) provides for state control over information flows: «Reaffirming the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news, which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, cooperation and friendly relations among States and nations, recognizing the duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States» [20]. Such wordings prioritise censorship and restrictions of information flow as a state function. It makes impossible to reach consensus with the countries, where pluralism of opinions is the fundamental principle of the organisation of state power.

In addition to that, the document includes thirteen subparagraphs, some of them are rewriting the provisions of the GGE reports of 2013 and 2015 [17; 18]. In the same time, it is politically incorrect, despite the lack of recognition by the rest of the states, to declare it as «set of international rules, norms and principles of responsible behaviour of the states» [20].

The simultaneous work of the two GGEs over one item unlikely will lead to the achievement of a compromise. The Global Commission on the Stability of Cyberspace (GCSC) was established by international think-tanks as an alternative platform for developing rules of responsible behaviour in cyberspace. The outcomes of GCSC is the «Singapore Norm Package» announced in November 2018 [5]. Despite the ambition of the project, the work of the Commission is not so meaningful. Most of the proposed «new norms» are derivative or narrowed formulas from the texts prepared by the GGE in 2013 and 2015 [17; 18].

What format is preferable for advancing international discourse over the creation of the global culture of cybersecurity? How to achieve common understanding and to build confidence in cyberspace? These and other questions are still open for discussion. Further research of the topic and discussions are required.

Conclusions. The international discourse around the core values and principles of developing global culture of cybersecurity is at an early stage and is essential for the emergence of a coherent position among international political actors on rules of responsible behaviour in cyberspace. By identifying the key factors of influence and the drivers of development, we can better understand the trends, both from the institutionalisation perspectives and composition of the principles that embody and protect universal values as a component of the global culture in cyberspace. It is premature to argue that there is significant progress in the regulation of the behaviour of states in cyberspace because, in order to achieve this, it is necessary to lay the international legal foundation, on which it is possible to create a global culture of cybersecurity. The lack of harmonisation of the positions (political will) of the states for the values fundamental to the development of the cybersecurity culture is a crucial problem in inhibiting the development of international legal cooperation in this area.

Література

1. An Internet Free and Secure. A human rights-based approach to cybersecurity. 2017. URL: https://freeandsecure.online (дата звернення: 18.01.2019).

2. ENISA. Cyber Security Culture in organisations / ENISA. 2018. URL: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport (дата звернення: 18.01.2019).

3. Fagerstrom, A. Creating, Maintaining and Managing an Information Security Culture. Degree Thesis. Information and Media Technology / Fagerstrom, Alex. 2013. 37 p. URL: https://www.theseus.fi/bitstream/handle/10024/63254/Fagerstrom_Alex.pdf?sequence=1 (дата звернення: 18.01.2019).

4. Finnemore M., Hollis D.B. Constructing Norms for Global Cybersecurity // The American Journal of International Law. 2016. 3, 110, 425-479.

5. GCSC. Singapore Norm Package. 2018. November. URL: https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf (дата звернення: 18.01.2019).

6. Guiora, A.N. Cybersecurity. Geopolitics, Law, and Policy / Gyiora, Amos N. Routledge. 2017. 170 p.

7. IGF. Main session: Enhancing Cybersecurity and Building Digital Trust // Proceedings from IGF'15. João Pessoa. Brazil. 2015. 10-13 November. URL: https://intgovforum.org/multilingual/content/2015-11-12-enhancing-cybersecurity-and-building-digital-trust-main-meeting-hall-finished (дата звернення: 18.01.2019).

8. Macron, E. Paris Call for Trust and Security in Cyberspace / Macron, Emanuel. 2018. 12 November. URL: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf (дата звернення: 18.01.2019).

9. Manjikian, M. Cybersecurity Ethics: An Introduction / Manjikian, Mary. Routledge. 2017. 232 p.

10. Osula, A.M., Roigas, H. International Cyber Norms: Legal, Policy and Industry Perspectives / Osula, Anna-Maria, Roigas, Henry (Eds.). NATO CCD COE Publications, Tallinn. 2016. URL: https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html (дата звернення: 18.01.2019).

11. Ross, S.J. Creating a Culture of Security / Ross, Steven J. ISACA. 2011. URL: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx (дата звернення: 18.01.2019).

12. Spinello, R. Cyberethics: Morality and Law in Cyberspace // Journal of Information Ethics. 2005. 14 (1). 70-90.

13. Schmitt, M.N. Tallinn Manual 2.0 on the international law applicable to cyber operations / Schmitt, Michael N. (Eds). Cambridge University Press. 2017. 598 p.

14. The UN Secretary General High-level Panel on Digital Cooperation. Call for contributions. 2018. 8 October. URL: https://digitalcooperation.org/call-for-contributions/ (дата звернення: 18.01.2019).

15. The UN Secretary General High-level Panel on Digital Cooperation. Responses to Call for Contributions. 2019. January. URL: https://digitalcooperation.org/responses / (дата звернення: 18.01.2019).

16. UNGA Resolution 57/239 "Creation of a global culture of cybersecurity". 2003. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf (дата звернення: 18.01.2019).

17. UNGA. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2013. URL: https://undocs.org/A/68/156 (дата звернення: 18.01.2019).

18. UNGA. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2015. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (дата звернення: 18.01.2019).

19. UNGA. The resolution "Advancing responsible State behaviour in cyberspace in the context of international security". 2018. URL: https://undocs.org/A/C.1/73/L.37 (дата звернення: 18.01.2019).

20. UNGA. The resolution "Developments in the field of information and telecommunications in the context of international security". 2018. URL: https://undocs.org/A/C.1/73/L.27/Rev.1 (дата звернення: 18.01.2019).

References

1. An Internet Free and Secure. (2017). A human rights-based approach to cybersecurity. Retrieved from https://freeandsecure.online. [in English].

2. ENISA. (February 6, 2018). Cyber Security Culture in organisations. Retrieved from https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport [in English].

3. Fagerstrom, A. (2013). Creating, Maintaining and Managing an Information Security Culture. Degree Thesis. Information and Media Technology. Retrieved from https://www.theseus.fi/bitstream/handle/10024/63254/Fagerstrom_Alex.pdf?sequence=1 [in English].

4. Finnemore M., Hollis D.B. (2016) Constructing Norms for Global Cybersecurity. The American Journal of International Law, 3, 110, 425-479 [in English].

5. GCSC. (November 2018). Singapore Norm Package. Retrieved from https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf [in English].

6. Guiora, A.N. (2017). Cybersecurity. Geopolitics, Law, and Policy [in English].

7. IGF. (10-13 November 2015). Main session: Enhancing Cybersecurity and Building Digital Trust. Proceedings from IGF'15. João Pessoa. Brazil. Retrieved from https://intgovforum.org/multilingual/content/2015-11-12-enhancing-cybersecurity-and-building-digital-trust-main-meeting-hall-finished [in English].

8. Macron, E. (12 November 2018). Paris Call for Trust and Security in Cyberspace. Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf [in English].

9. Manjikian, M. (2017). Cybersecurity Ethics: An Introduction [in English].

10. Osula, A.M., Roigas, H. (Eds.) (2016). International Cyber Norms: Legal, Policy and Industry Perspectives. Retrieved from https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html [in English].

11. Ross, Steven J. (2011). Creating a Culture of Security [in English].

12. Spinello, R. (2010). Cyberethics: Morality and Law in Cyberspace [in English].

13. Schmitt, M.N. (Eds). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations [in English].

14. The UN Secretary General High-level Panel on Digital Cooperation. (8 October 2018). Call for contributions. Retrieved from https://digitalcooperation.org/call-for-contributions/ [in English].

15. The UN Secretary General High-level Panel on Digital Cooperation. (January 2019). Responses to Call for Contributions. Retrieved from https://digitalcooperation.org/responses/ [in English].

16. UNGA (2003). Resolution 57/239 "Creation of a global culture of cybersecurity". Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf [in English].

17. UNGA (2013). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from https://undocs.org/A/68/156 [in English].

18. UNGA (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [in English].

19. UNGA. (2018). The resolution "Advancing responsible State behaviour in cyberspace in the context of international security". Retrieved from https://undocs.org/A/C.1/73/L.37 [in English].

20. UNGA. (2018). The resolution "Developments in the field of information and telecommunications in the context of international security". Retrieved from https://undocs.org/A/C.1/73/L.27/Rev.1 [in English].

Стаття надійшла до редакції 25.01.2019 р.