UDC 325.744

Volodymyr Grubov

Doctor of Political Sciences, Professor, Leading Researcher of the Research, Center for Humanitarian Problems of the Armed Forces of Ukraine, Kiev

e-mail: GrubovVM@gmail. com

Mykola Sanakuiev

PhD in philosophical science, senior lecture of the Department of advertising and public relations, Institute of journalism, Borys Grinchenko Kyiv University

e-mail: m.sanakuiev@kubg.edu.ua

INTERNATIONAL SPACE INFORMATION: CONFRONTATIONAL REALITY OR POSSIBILITY OF DIALOGUE?

Abstract

The article is an attempt to find the key problems of political and legal settlement of the international information space through a combination of methodology for its determination and the interests of the leading players interacting on the site of the UN.

Tectonics changes that brought the global politics of information considered in the contest birth of a new objective reality and causes that produce it — is the existence of «axial» principles of organization of information being human (D.Bell), the struggle between the «national and international society» and national conflicts security strategies of the leaders of world politics.

This policy is based within the familiar concept of «real politic» (G. Morgenthau), which is in first place in international relations was not the principle of law and the principle of power «struggle for power levers» that demonstrated the willingness of the strongest members of the world order to apply hybrid methods of struggle. It is emphasized that this trend raises a number of negative consequences both social and political, legal and humanitarian aspects in the life of individual societies, as entire countries.

It has been suggested that the level of severity of the political and legal conflicts in a more equitable manner in the functioning of the information-mesh postoru depend on how consistently the main players in world politics will follow conventions already achieved, and not worry about persecution own benefit and interest.

It is emphasized that the language of political practice, this means that democratic slogans proclaimed human rights objective information and privacy began to sink in organized public and private information violence, and it was just part of the language semantics television, texts newspapers and magazines, daily communication.

It is proved that a similar situation shows the existence of a conflict between the constant declarations of priority of rights and freedoms and the growth opportunities of interested residents to control the information space «information man». This conflict is present in the information policy of virtually all world leaders.

In the context of identified internal contradictions and the increasing severity of humanitarian problems analyzed complex problems of political and legal nature that need to be addressed to the international community both within the political and legal relations that exist in the UN system for information policy and within the established concept of «soft security» (soft power), which now attracted the leading countries of the world.

Keywords: information space, international information space, information security, cyberspace, strategy, national interests, conflict.

УДК 325.744

Грубов Володимир Михайлович

Доктор політичних наук, професор, провідний науковий співробітник, Науково-дослідний центр гуманітарних проблем Збройних Сил України

e-mail: GrubovVM@gmail. com

Санакуєв Микола Георгієвич

Кандидат політичних наук, старший викладач кафедри реклами і зв'язків з громадськістю, Київський університету ім. Бориса Грінченка

e-mail: m.sanakuiev@kubg.edu.ua

МІЖНАРОДНИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР: КОНФРОНТАЦІЙНА РЕАЛЬНІСТЬ ЧИ МОЖЛИВОСТІ ДІАЛОГУ?

Резюме

Метою статті є спроба знайти вузлові проблеми політико-правового врегулювання функціонування міжнародного інформаційного простору на основі поєднання методології його визначення й інтересів провідних гравців, які взаємодіють на площадці ООН.

Для досягнення мети були використані такі методи: діалектичний, системний, аксіологічний, компаративний.

Результати. На основі викладеного матеріалу висловлюється думка, що у сучасній політиці врегулювання міжнародного інформаційного простору досить чітко проглядається декілька ключових проблем. Першою проблемою є визначення поняття «інформаційного простору» та ключових питань його функціонування, що ми спостерігаємо на національному рівні. Другу проблему уособлюють головні тренди світового інформаційного простору. З одного боку, спостерігається зацікавленість країн-членів ООН щодо більш тісної співпраці у питаннях кореляції міжнародного і національного сегментів правової політики щодо врегулювання інформаційної діяльності між її суб'єктами, а з другого, — де-факто, простежується протистояння між країнами-лідерами світової інформаційної потуги та їх намірами нав'язати свою волю решті світової спільноти, яку утворюють країни аутсайдери, але вже на новому полі глобальної гри. Це чітко проявляється між такими інформаційними гігантами нового століття (у самому широкому значенні цього слова) якими є США, Китай і Російська Федерація. На додаток ситуацію неврівноваги посилює фрагментарна і надто обережна лінія поведінки ООН і МСЕ відносно позиції цих країн. Ці та інші чинники створили ситуацію, коли незважаючи на цілу низку рішень у цьому важливому питанні, ООН так і не наблизилася до вироблення дієвого міжнародного документу, на який погодилися б всі її країни-учасниці.

Ключові слова: інформаційний простір, міжнародний інформаційний простір, інформаційна безпека, кіберпростір, стратегія, національні інтереси, конфлікт.

1. Introduction

The fact of our day is that the transformation of scientific — technical progress taking place on the basis of knowledge and innovation has become a « high level chimera» where the informative resource is unidimensional assessment of power of the country and its latent possibilities to change any negative circumstances in their favor. In international relations conservation of this reality into information technology benefits determines the growth of regressive processes which are largely dependent on the same reality. Today its logical foundations demonstrate two dominant global trends: 1) leverage forces that have information culture leaders demonstrate the weakness of those who are outside of mainstream and 2) with the development of ICT information legal personality is

lost as a basis for legal regulation of information space — a place of many providers of information communication. Such tendencies inherent both within individual countries and for the global network community as a whole. Internet capabilities and information technology has become a kind of negation of the existing order of things, and «all the successes of reason, according to F.Junger, became products of sphere of reason» [1, p. 163]. Recognition of this fact shows that the problems of legal culture of the information communication become transboundary and global. This gives some reason to believe that the great humanistic ideals represented by theorists of paradigm of the information society lose its integrity and humanistic unilinearity of dominant information culture. As the phenomenon of the human mind today inherent logical contradiction with deeper meanings and purposes. They personified in national mentality, national interest and information policy of the state as a resource of national affirmation.

2. Research methods

Analysis of the latest sources and publications shows that since the mid 90-ies these reasons identified problem field and agenda of major international policy areas where the issues of the global information society and security implications of traditional information-vulnerable culture [2]. Under the close supervision of politicians, spin doctors and various think tanks were such phenomena of the information society as «mosaic structure of culture» and «global metropolis» (H.Kahn, E.Wienner), « audio-visual communication», «mass culture» and the «end of political ideologies» (Z. Brzezinski, M. McLuhan), «global embrace» and «global village» (M. McLuhan, A.Toffler) «cyberspace» and «cybersecurity» (M.Benhemann, F. Machlup, Y. Hayashi), etc.. On the one hand as apologists and critics of technocracy waves they pointed to technological reasons of socio-economic, socio-political, spiritual and cultural changes that are expected in the future world civilization, on the other, revealing Unity — interposition character that these processes are in the international community, they pointed out that in managing global processes Information technologies become strategic importance [3]. Domestic scientists also touch the subject. O.Dzoban, V.Shtanko, L. Tikhonov et al. displayed the nature of these strategies and particular methods of their implementation at the present stage of international information space in the socio-cultural aspects, cybersecurity aspects — D.Dubov, M.Ozhevan V. Sadovnichiy, I.Lazarev, M.Beylin et al., international legal aspects — A.Chernova, A.Huz, V.Pylypchuk and others. However, despite the rather wide range of research in this topic, the problem of political and legal settlement of international information space in the international information policy retains its «areas of concern» and still not covered.

The purpose of the article is an attempt to find the key problems of political and legal settlement of the international information space through a combination of methodology for its determination and the interests of the leading players interacting on the site of the UN.

For this purpose, the following methods were used: dialectical, system, axiological, comparative.

3. Results and discussion

One of the first drew attention to the consequences of the global nature of information and information technology was D.Bell. Tectonics changes they have brought and can bring in future life, he connected with a new objective reality as a result of the materialization of certain reasons.

The first group of reasons D.Bell considered in the context of the «axial principles. » Considering society as the interaction of three areas: social (feasibility), political (political system of society) and culture, he pointed out that these systems are characterized by some peculiarities of control. These features are based on the «axial principles». So the economy is guided by efficiency, political system — the principle of equality, and culture — the self-identity principle. In capitalist society through very different life opportunities of the individual, says Bell, lack of unity between these spheres is the source of all disputes Western lifestyle [4].

The second group of reasons is determined by struggle between the «national community» and the «international community. » The problem here is in competition philosophical principles of international law subjects, e. g. individual states. In pursuit of their own interests they destroy the old political and legal norms of international order and promoting the idea of globalization provide updated international legal registration of international infrastructure. Through this process of the international community will not look like an organized international order but rather as amorphous space-time integrity, which caused global character of communication.

The third group of reasons rooted in competition in the media sector as the most profitable activity of private capital interests and interests of the state that the strategy of national self-assertion on the inside — and foreign levels perform regulatory, organizational and control function [5].

The fourth group of causes rooted in the national strategies of the leaders that since the 70s of the last century in international relations highlighted as a key factor information. With unlimited opportunities of information resource and vulnerability of the human mind by cascade of information flow, national governments, pursuing certain interests, began to implement targeted actions to create artificial consciousness for information consumers both inside and outside the national territory. Mainly these interests concentrated in the military, political and economic sphere and the success of their achievements associated with the chosen strategy.

The strategy is a systemic view of politics, administration and the war (which almost never ended, but only modified forms of reference: war (fighting) in economic and informational wars between countries). It must be said that in this sense, the strategy advocates as the art of resource allocation in order to gain advantages in the struggle and achieve specific policy objectives at the lowest cost. [6] That is the picture we see today in international relations when through the transformation of the force factors, the world is becoming more «heterogeneous. » However unlike in the 60–70-ies its «heterogeneity» as R.Aron wrote [7], determine not only the classic force factors that tend to the natural physical factors but the scope of reason that produces a «thinking tool that is used for human exposure» [8, p. 160].

In the world of human realities of the information age this recognition took place within already familiar to the general public the concept of «real politic» (G. Morgenthau), which is in first place in the international system recognizes no principle of law and the principle of power «struggle for power levers» which demonstrated the willingness of the strongest members of the world order to use hybrid methods of struggle. Unlike geopolitical reformatting the political map of Europe that occurred in the 90s of XXth century, «classic» power struggle waged between the leading actors of world politics, today it follows the logic of «soft power» on the basis of information and democratic tools. Word and mediated action considered an ideal key to the practical solution of any problem where there is a human mind. So the best form of influence is the one through which the partner or opponent transforms the secret meaning of his intentions on the opposite side as their own non-alternative and most efficient action in the situation emerging or developed for it. This way, the partner of dialogue unwittingly chooses the wrong course of action, which another mind imposed [9, p. 20–26]. The purpose of this struggle is the destruction of geographic hierarchies of social experience and cultural archetypes as a form of knowledge and replacing them with «new and more progressive» evaluation tools reality.

Another negative consequence caused by increasing global communication process is the erosion of nominal power holders in sovereign countries and gradually transfer real power to the centers of preparation of solutions that are abroad. According to the laws of the organization of the information environment the winner in the political and economic struggle is the one who is more capable of collecting, processing and disseminating information. This mechanism of communication gradually forms the system of superpower, based on the information superiority, and its inalienable characteristic is its concealment and influence on the audience [10, p. 621]. n terms of evaluating the effectiveness of foreign policy strategy this is considered the key actions and informational space in this task serves as single-option policy resource.

In the set of information relations «information space» is the basic concept of information law. However, despite its apparent clarity, there is hidden game of human rationality in combinftion of two words «space» and «information» from the very beginning. This makes it impossible to use traditional concepts of space of information relationship, need another look at this phenomenon. Here are some examples of definitions of information space. The version of the «eEurope», which was launched in March 2000 in the EU Information space is defined as: 1) Integral electronic information space that is created using electronic networks; 2) Areas in modern public life of the world in which information communications play a key role. (In this sense, the concept of information space close to the concept of information environment).

These definitions reflect the purely technical side of the concept of information space and subjugated above all, to the united Europe initiatives to achieve key objectives:

• bring digital technology and the Internet to every citizen, in every home, school, businesses and public institutions;

• overcome the digital «illiteracy» in Europe through culture of entrepreneurship, open to the use of new information technologies;

• ensure social loyalty information society.

Researcher A.Chernov gives the following definitions: 1) information space — a territory within which information flows occur; 2) information space — a resource that is used legal and non-legal entities for their own purposes; 3) information space — an environment in which there are information resources (here resource information means actual information); 4) information space — is the sphere of information relations emerging between different actors on the production, distribution and use of information. [11]

The first three definitions of the information space is capacious enough and those that primarily focus on technical and technological aspects of its operation.

If the information space is considered as a territory, its characteristic features are: the borders (national, regional, supranational, real, virtual, symbolic, rigid flexible, etc.); Length (interrupted, not interrupted, discrete, etc.).

If the information space means the resource, it is possible to isolate the following characteristics: information potential (low, high, uniform uneven); Information infrastructure (an organizational structure that provides the functioning of the information space; means that provide access to information).

The information space as an information dissemination environment, it is characterized by: the potential of such a resource as information (information services, various software products); Density, boundaries and length of space, where information resources are located.

Consequently, the proposed variants of definitions have many features of the information space, but these definitions lack the main thing — they lack the subjects of information relations, as carriers of a certain mentality and ideological culture. This indicates that the scope of these definitions can not be universal, it is limited mainly to the technical and technological spheres.

In the framework of the social system and international relations, where various institutes, structures, cultures and racial characters interact (G. Lebon), the definition that the information space — a sphere of information relations that arise between different actors in relation to the production, distribution and use of information is more acceptable due to the fact that it defines subjective — object and spatial boundaries of communication. This definition allows to identify:

1. Subjects of the information space according to any given criteria. In this case, it is important to determine the following characteristics: the behavior of subjects (their goals, motives, interests, belonging to different information groups, legal status); Interaction of subjects through information institutes; The hierarchy of relations between actors and the information space; Informational mobility of subjects.

2. The object of the information space — information. In this case, the analysis subject is: material media of information (their forms, types, etc.); resource potential (price, utility, relevance,

interchangeability with other resources); access of subjects to information; distribution of information between different actors.

3. Field of interaction of information subjects (its boundaries, length, density, national-cultural character, etc.).

4. Features of linguistic culture (linguosphere — linguistic concept of the world, the logosphere-concept, category, formation of the national linguistic network within the «multilingual society»).

5. Features of the psychological «map of the world» of ethnic groups (archetypal thinking, mentality).

Such an approach to the content of the notion of «information space» is recognition of the fact that there is acertain logic in the organization of the information space of an open society. Despite national peculiarities in world practice, there are three main components: 1) the identification and definition of the rights of various categories of users; 2) classification of categories of users according to the regime of preservation of state and commercial secrets; 3) determination of the boundary of the internal and external information circulation space of information [12].

Remaining a dynamic and universal system, the information space always acts as an all-inclusive towards its national and other diverse subjective practices and their variations. This allows it to acquire the characteristics of substantiality and: 1) act as a form of social consciousness, the main feature of which is infinity in time; 2) to be in a permanent state of incompletion, because the subjects of communication constantly increase the volume of various information; 3) to be in a state of heterogeneity, because it has attraction attracting attention and barriers that displace the consumer's attention from this point of the information space; 4) to act as a product of public opinion and to form a public opinion; 5) demonstrate national-specific ways of constructing, processing and disseminating information [13, p. 152]; 6) rather remain semi open, than open, because its use as an «eternal» resource always dictates interest.

An excursion into understanding the essence of the informational space, which modern methodologygives, pushes to the thought: the level of acuteness of political-legal conflicts in its components will depend on how actively and consistently residents of this space will pursue their own benefits and interests. As the events of the last 15 years of the XXI century show, leading players in the world's information space are primarily concerned with the protection of the information space and information sovereignty. At the language of political practice, it began to mean that the proclaimed democratic slogans on human rights for unbiased and objective information and the inviolability of private life began to lapse in organized state and private informational violence. And it became part of the language, the semantics of television broadcasts, the texts of newspapers and magazines, daily communication. This situation reflects the existence of a conflict between the constant declaration of the priority of human rights and freedoms and the growing opportunities for interested residents of the information space to control the «information man». The freedom of information and the openness of the information space are in a deadlock of history, and the history once again «laughed» over this freedom. And paradoxically, this happened in the United States as an example of democracy, where President D.Tramp publicly described the US media as «enemies of the American people» at a media briefing in February 2017. The list was headed by such well-known information corporations as CNN, NBC and CBC, which until recently considered world standards for the art of providing information.

Consequently, in the definitions of the information space and understanding of it either as a «resource» or as a «field» reflects a deeper in content perspective. Its shadow and variational manifestations are particularly contrastingly followed in the existing international discourse on this issue, whose purpose is to impose to the audience its existing or forming view on informational reality. It may be elections, war, politics, art, etc. The tactics of constructing discourse always follow the main rule: the dominant discourses, in order to survive, must impose the values that they proclaim through repetition, strengthening and materialization. First of all, the implementation of this rule contributes already articulated in the information space values (positions), which on the surface do not cause particular questions. From the point of view of the problems of functioning of the international in-

formation space such established discursive issues in the broadest sense are 1) information security of the state; 2) information security of the individual; 3) cybersecurity; and 4) strengthening trust and security in the use of ICTs. However, in the language of information policy and practice of almost all countries, these issues acquire a national-specific sound and are mainly understood in the categories of «confrontation», «struggle» and «defense» from external interferences and influences. Changing the context of new modalities affects the change in interstate informational and security discourse. Today the dominant issues are the theft prevention and protection of information, ensuring the integrity and functionality of the information infrastructure, database protection, the neutralization of destructive information, monitoring of the national information space and its legal protection. Such a reaction is evidence that, with the growth of the information power of world leaders, security issues become important in the plane both in the open and in the closed agenda. Accordingly, it pushes the institution of the state to strengthen its activities in this direction. According to the expert community, this line of behavior is dictated by a new information reality, which is defined by: the challenges and threats associated with the use of information resources (information and psychological operations, information aggression, cyberterrorism, cybercrime, advertising, computer games, etc.), the danger of manipulation the human consciousness and the growth of the scale of this phenomenon, the consequences of the use of information weapons that are equivalent to the consequences of the use of weapons of mass destruction, the legal vacuum at the national and international-legal levels in the legal regulation of actual issues of information security and the functioning of the information space [14, p. 236–237].

First of all, this is due to the information rivalry and the complexity of regulation of information relations both at the interstate and non-state level, which form various subjects of information relations. In the international information space, the main ones are information transnational corporations such as Microsoft, Google, Yahoo, Facebook, Youtube, Apple, etc., which, with the support of the state, pursues not only commercial but also far-sighted goals of the «great policy» of the state itself. In this symbiosis, the phenomenon of «functional thinking» by F. Junger is viewed. «There is a force in it that promotes the propagation and spread of automatism... There is an aggressive grip, the ruthlessness that few people fully realize. It is one of the coldest inventions of rational mind, which manages technical progress « [8, p. 133]. Such a view of F. Junger makes us look at the information technologies and the way of thinking that they form as an instrument that «transforms a person into a system of functions», a cog in a state machine that controls its own information space. As the information law practice shows, the closed agenda of the information security issue transforms this trend into the norm of life of information communities. An example of such a reality is the information security policy of the United States, the Russian Federation (RF) and China, which is conducted by these countries in the information space of national jurisdiction. Without going into detail, we note that for the state as an instrument of violence, which possesses information technologies, this space has long been «absolutely transparent». Accordingly, there is almost no place for «secrets» of an individual person in it [15; 16; 17; 18; 19; 20; 21].

In this context becomes clearer the entire complex of ethical and legal issues that need to be addressed to the international community within the framework of the political-legal relations existing in the UN system and within the newly-formulated concept of «soft security», which is popular today the United States. Due to the dominance in the field of information and communication technologies (ICTs), they seek to transform the world «for themselves» and, accordingly, impose the rules of the game on the world community, which will satisfy only one side. But despite the leading role of the United States in the US-Russian-China information and power relations triangle, they are unable to achieve this goal for a number of reasons. Their content defines the disagreement between the RF and China regarding US approaches, first of all, to resolve issues that are critical in terms of advancing national interests in the field of cybersecurity. In contrast to the United States, Russia and China regard cybersecurity not as a separate sphere but as a component of national information space. Hence, the main reasons that hamper US, Russian and Chinese cooperation in the security information sphere today are that: Due to the dominance in the field of information and communication technologies

(ICTs), they seek to transform the world «for themselves» and, accordingly, impose the rules of the game on the world community, which will satisfy only one side. But despite the leading role of the United States in the US-Russian-China information and power relations triangle, they are unable to achieve this goal for a number of reasons. Their content defines the disagreement between the RF and China regarding US approaches, first of all, to resolve issues that are critical in terms of advancing national interests in the field of cybersecurity. In contrast to the United States, Russia and China regard cybersecurity not as a separate sphere but as a component of national information space. Hence, the main reasons that hamper US, Russian and Chinese cooperation in the security information sphere today are that: — Russia and China do not recognize the Cybersecurity Strategy (2011), which the United States has proposed to the international community as the basic documentation on the basis of which it would be possible to sign an international agreement that would regulate the main provisions of the activities of residents of international information policy. — Russia and China are opposed to the US concept of «free flow of information», on the basis of which it is necessary to build a large Internet. In their view, such a principle denationalises the information space in favor of the United States and ICANN, which is under its control, which today is the only entity that controls its activities. Russia and China support the transfer of control function over the Internet to the United Nations (or ITU) [22, p. 190–191]. — The United States deliberately and consistently advances the view that the documents they are presenting on international sites, where issues of information security are discussed, are universal in nature and in accordance with the UN proclaimed principles of human rights and freedoms.

Proceeding from the context of the contradictions between the main players in the international information space, these problems can be considered in two ways: how to preserve the sovereignty of the state in the information space in the conditions of global technocracy and information openness, and how to built a fair world information society, which would take into account the interests of all countries?

Today in the system of international relations not only otransboundary threats, such as international crime, terrorism and terrorist activity in cyberspace cause concern, but also the possibility of the use by individual states of ICT for purposes incompatible with the goals of ensuring international stability and security. Equally dangerous is the resistance of individual countries (groups of countries) to internationally adopt an international legal instrument with statements of threats to international information security and their neutralization in the interests of the entire international community. It is appropriate to bring two points of view, which show the complexity of this issue on the UN site: one concerns the United States, and the other — Russia. For example, US Sen. M. Romney, articulating with cybersecurity issues, expressed his opinion on «the need to build such US armed forces, which no country in the world will be able to challenge». And the head of the Interdepartmental Commission on Information Security of Security Council of the Russian Federation, V. Sherstyuk, accused the United States in «the creation of special units, cyber command, intended to carry out a military confrontation in the global information infrastructure» [22, p. 176–177].

The internationalization of the security discourse of the information space, which began since the late 1990s within the First Committee of the General Assembly of the United Nations on disarmament and security issues, has made it possible to clarify the positions of the participating countries in the field of information and security and to narrow substantially the greater part of the above-mentioned issues. Today,it is determined by the following issues: the discrepancy between the new opportunities that the information revolution has for international cooperation, peace and security and the political goals pursued by individual countries; the need for coordinating the actions of the international community in combating new transboundary threats connected with the use of ICTs; prevention of the emergence of information wars between states and the deployment of information weapon systems; preparation of an international agreement on information security [23, p. 477–479]. Summarizing the content of the adopted documents that have been adopted within the UN for the last 15 years, it should be noted some key issues that have caused the most heated discussions and which still fail to reach common solutions.

The most controversial issue on the UN site remains the question of using ICT for military-political purposes and the creation of systems of information weapon. The key difference lies in the fact that the United States and its allies are of the opinion that only the issue of cybersecurity (techno-technological component of security, sometimes called an instrumental component) should be considered at the international level, leaving the issue of informational and psychological influences outside the discussion field. The position of China, the Russian Federation and the countries supporting them is based on the fact that behind the instrumental component there are always the hidden interests of the subjects of the information space that pursue economic, political, social and military goals. Hence, in contrast to the United States and its allies in the context of possible agreements, an acceptable option for them is the formulation of documents instead of cyber security categories in categories of information security (international information security). As the researcher of this question, D. Dubov states, «most UN documents operate with the concept of» international information security « (IIS), with the utmost caution filling it meaning. As a result, the concept that the UN uses, looks if not as a compromise between the two alternatives, then at least as such, which may lead to the aforementioned compromise « [22, p. 160].

At the United Nations in December 1998 by the UN General Assembly Resolution A / RES / 53/70 was reflected the problem of a new reality that the international community began to perceive as «soft security» that one country owned. The resolution noted that the dissemination and use of information technology and tools affected the interests of the entire international community. The resolution expressed concern that these technologies could potentially be used for purposes incompatible with the objectives of international stability and security [24]. Hence, the main modalities of the Resolution and all UN documents contained only the expectation that the member states will understand the growing problems. Subsequently, the raised issues were reflected in United Nations General Assembly Resolutions A / RES / 54/49 (1.12.1999) and A / RES / 55/28 (20.11.2000). But in their content they repeated the previous document and only contained an appeal to the world community to fulfill the agreements already reached.

The position of the United States in the issues of «inviolability» of its own cyber-field [25] and in the high interest of the fastest international legal settlement of this issue on its conditions reminds the position of «tired sprinter», who made a jerk and outstripped all participants,but began to feel tired and anxiety that rivals will outstrip him. The chances of US adversaries to schift America from leadership positions are based on the phenomenon of rapid internationalization of science and the availability of knowledge that is becoming the basis of new technologies. Freedom of movement of knowledge and IT specialists, what so dreamed the apologists of the free market, turned them into a challenge with many unknowns, where, besides money, there are ambitions, adventure, spiritual searches and much more that is not subject to rationalization.

But the most unpleasant fact for the US is the publication in March 2017 of a well-known WikiLeaks project of documents related to the activities of a group of hackers working under the «roof» of the CIA at the Center for Information Collection, based in Frankfurt am Mein (Germany). Almost the US has been accused of leading a global cyberwar «against all» and even against its allies. In this situation, the United States proved to be a violator of the «ethics of global cyber security». As a party to the international cyberspace problem resolution process, the United States signed its signature under documents such as United Nations General Assembly Resolution A / RES / 55/63 (4.12.2000) «Fighting against the criminal use of information technology», A / RES / 56/19 (29.11.2001) «Achievements in the field of informatization and telecommunications in the context of international security», A / RES / 57/239 (December 20, 2002) «Creation of a global culture of cyber security», etc. The resolution part of these documents drew the attention of national governments to taking measures at the national level aimed at counteracting cybercrime; strengthening cooperation between law enforcement agencies; optimization of the system of protection of personal data, information systems of electronic data; raising public awareness about the new challenges of the information society; Bringing people to the global culture

of cyber security, whose components are awareness, responsibility, response, ethics, democracy, risk assessment, security management, reassessment (reassessment of security values).

Violating the content of the above-mentioned Resolutions, United States has practically demonstrated to the whole community that the US national interests are not in accordance with the UN resolutions, which America regards superficially, but with the information reality that has emerged today. On the one hand, America defines it, and secondly, it contains threats to its domination. In the words of former US president B.Abama, America will never share achievements in digital infrastructure, which is a «strategic national value,» and in cybersecurity terms it will be «protected by a national priority» [26].

The second major issue in the UN area remains the issue of extraterritorial management of the Internet. Today, the United States, as the founding country of this global project, practically owns all the rights to regulate it. Actual monitoring of the technical part of the network is provided by ICANN Corporation and the IANA (Internet Assigned Numbers Authority), which are closely linked to US government agencies. The fundamental moment of this issue is that ICANN retains control over DNS root domains (Domain Name System), through which the Internet is predominantly routed. The technical standards of the Internet are also established by two other companies located in the United States IETF (Internet Engineering Task Forse) and IAB (Internet Architecture Board) [22, p. 168].

The United States explain its position on sole control over the Internet by the first amendment to the US Constitution, which equates freedom of information with the basic principle of democracy: without this freedom, no society can be regarded as «free». Therefore, there are no «reasonable» restrictions on restrictions on freedom of information and expression, since it is unlikely that everyone would be able to agree on what mean «reasonable» restrictions. Even the discussion of this idea is a form of regulation of freedom. Therefore, the protection of the freedom of expression must be absolute and not restricted. From the position of the United States, this freedom can only be provided by US information policy, which tool is the Internet.

The European concept, supported by China and Russia, is based on Article 10 of the European Convention on Human Rights, which emphasizes the fact that there can be no freedom (and, therefore, the expression of opinions) without adequate responsibility. In this way, the convention justifies some of the actions of governments regarding the legislative regulation of this sphere of public relations.

At the UN, these two approaches to freedom of speech and opinion become a form of prolonged confrontation, which is interwoven with a variety of international decisions, recommendations and resolutions. Discussions around this issue that took place after the Tunis summit (2005), WWRIS — 2006, Athens (Greece); 2007, Rio de Janeiro (Brazil); 2008, Hyderabad (India); 2009, Sharm el-Sheikh (Egypt), etc., showed that the issue of ensuring the vitality and security of the network's operation, the formation of a dialogue environment between the public bodies dealing with issues of international policy on the Internet, the strengthening of the cooperation of intergovernmental organizations, whose competence is the functioning of the Internet etc. The world community connects the UN and the ITU (International Telecommunication Union). The key role of the ITU member countries has been to strengthen confidence and security within the union and to develop concrete measures to curb cyberthreats and insecurity in the information society [27].

Such formulation of the issue means deprivation the US of leading role in the definition of the subject of information world flows and the gradual formation of a consensus-based form of government from a «single center», which can be either a specially formed body with the UN or ITU. The launch of the new global network management policy was the establishment of an Internet Governance Forum (FOI) in November 2006 (Athens). The reluctance of the United States to see the phenomenon of global democracy on the Internet was an open demonstration that the views of the United States contradicted the principles proclaimed at the World Summit on the Information Society and the United Nations Millennium Declaration (2000). This shows that the development of the political and legal foundations of international information security is too complicated and controversial issues of international politics. The world community faces the conservative Height politic, which is based on such

traditional categories as national interests and the struggle for power. This is also fully relevant to the information sphere. So today, compromises and goodwill of the governments of the UN member states are required to comply with documents already adopted and to facilitate the establishment of more open and honest cooperation for the good of all in the information sphere.

4. Conclusions

In the current policy of regulating the international information space, two trends are clearly visible.

On the one hand, there is an interest of the UN member states in closer cooperation, and on the other hand, there is de facto traced the confrontation and the attempts of leaders to impose their will and their vision on others. The unbalanced situation is aggravated by the fragmentary and overly cautious UN and ITU line of conduct.

Despite a range of decisions on this important issue, the UN is still far from developing an effective international instrument that would be of interest to all.

5. References:

1.Shkepu M.A. Arhitektonika obschestvennogo vremeni: monografiya. — K.: KNTEU, 2012. — 334 s.

2. Ataka na razum / Albert Gor; [per. s angl. A. Bogdanova i K. Minkovoy, pod red. Yu. Akimova]. — SPb.: Amfora. TID Amfora, 2008. — 478 s. — (Seriya «Lichnoe mnenie»).

3. Chugunov A.V. Teoreticheskie osnovaniya kontseptsii «Informatsionnogo obschestva». — SPbGU. SPb, 2000. — 52 s.

4. Bell D. Gryaduschee postindustrialnoe obschestvo. — Moskva: Akademiya, 1999.

5. Bell D. Sotsialnyie ramki informatsionnogo obschestva // Novaya tehnokraticheskaya volna na Zapade. — Moskva: Progress, 1986.

6. Sun-Tszyi. Iskusstvo strategii. — M.: Aspekt-Presss, 2008. — 477 s.

7. Aron R. Mir I vIyna mIzh natsIyami. — K.: YunIvers, 2000. — 685 s.

8. Yunger F.G. Sovershenstvo tehniki. — SPb.: VLADIMIR DALЬ, 2002.- 553 s.

9. Gart L. Strategiya. — M., 1956. — 456 s.

10. GlobalIzatsIya I bezpeka rozvitku: MonografIya / BIlorus O. G., Luk'yanenko D. G. ta In.; kerIvnik avt. kolektivu I nauk. redak. O. G. BIlorus. — K.: KNEU, 2001. — 733 s.

11. Chernov A. Stanovlenie globalnogo informatsionnogo obschestva: problemyi i perspektivyi//http://www. isn. ru/public/Book. zip.

12. Guz A.M. IstorIya zahistu InformatsIYi v Ukrayini ta provIdnih kraYinah svItu. K.: KNT, 2007. — 260 s.

13. Dzoban O.P. InformatsIyna bezpeka u problemnomu polI sotsIokulturnoYi realnostI: MonografIya. — H. Maydan, 2010. — 260 s.

14. Pilipchuk V.G., Dzoban O.P. InformatsIyne suspIlstvo: fIlosofsko-pravoviy vimIr: monografIya. Uzhgorod: TOV «IVA», 2014, — 282 s.

15. Beylin M.V. Novyie tehnologicheskie ugrozyi informatsionnoy bezopasnosti lichnosti// Chas viboru: vikliki InformatsIynoYi epohi: kolektivna monografIya/za zag. red. O.A. IvakIna, D.V. Yakovleva. — Odesa: VidavnichIy dIm «Gelvetika», 2016. — 472 s.

16. Furashev V. Proekt Wikileaks ta yogo sutnIst // Komuflyazh # 2. — 2011.

17. Elektronnyiy kontslager: po etapu idet «Eshelon»// «Russkiy vestnik». — 2003. — # 14. — [Elektronnyiy resurs]. — Rezhim dostupa: http://www. h-libri. ru/elib/smi01405/00000001.html.

18. Suleymanov S. Sledim strozhe chem za russkimi/ S. Suleymanov [Elektronnyiy resurs]. — Rezhim dostupa: https:// lenta. ru/ articles/2013/06/01/ bigbro/.

19. Pozhidaev E. Instrumentariy totalnoy slezhki i sovremennaya sistema kibershpionazha/ E. Pozhidaev [Elektronnyiy resurs]. — Rezhim dostupa: https:// regnum. ru/ news/1683920 html.

20. Leonov S. Eto holodnaya voyna? Rossiyskim chinovnikam zapretili polzovatsya servisami Google / S. Leonov [Elektronnyiy resurs]. — Rezhim dostupa: https:// ura. ru/ news/105185439.

21. Ivey Van. Kitayskaya model razrushaet gegemoniyu «obschechelovecheskih tsennostey» [Elektronnyiy resurs]. — Rezhim dostupa: http://inosmi. ru/ world/20130114/204595110.html.

22. Dubov D.V. Kiberprostir yak noviy vimir geopolitichnogo supernitstva: monografIya/D.V. Dubov. — K.: NISD, 2014. — 328 s.

23. Sovremennaya mirovaya politika: Prikladnoy analiz / Otv. Red. A.D. Bogaturov. — M.: Aspekt-Presss, 2009.- 588 s.

24. Globalizatsiya i bezpeka rozvitku: Monografiya / BiIorus O. G., Lukyanenko D. G. ta in.; kerivnik avt. kolektivu i nauk. redak. O. G. Bilorus. — K.: KNEU, 2001. — 733 s.

25. Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoy bezopasnosti: doklad Generalnogo Sekretarya OON [Elektronnyiy resurs]. — Rezhim dostupa: http:// www. un. org. /ru/ documents/ods. asp?m =A/RES /53/70

26.Cyber Storm Securing Cyber Space Rezhim dostupa: http:// www. dhs. gov / cyber-storm-securing-cyber-space.

27. Remarks by the President on securing our nations cyber infrastructure Rezhim dostupa: http:// www. white house. gov/the_press_offise/Remarks-by-the-President-on-Securing-Our-Nations Cyber-Infrastructure.

Література:

1. Шкепу М. А. Архитектоника общественного времени: монография. — К.: КНТЕУ, 2012. — 334 с.

2. Атака на разум / Альберт Гор; [пер. с англ. А. Богданова и К. Минковой, под ред. Ю. Акимова]. — СПб.: Амфора. ТИД Амфора, 2008. — 478 с. — (Серия «Личное мнение»).

3. Чугунов А. В. Теоретические основания концепции «Информационного общества». — СПбГУ. СПб, 2000. — 52 с.

4. Белл Д. Грядущее постиндустриальное общество. — Москва: Академия, 1999.

5. Белл Д. Социальные рамки информационного общества // Новая технократическая волна на Западе. — Москва: Прогресс, 1986.

6. Сун-Цзы. Искусство стратегии. — М.: Аспект-Прессс, 2008. — 477 с.

7. Арон Р. Мир і війна між націями. — К.: Юніверс, 2000. — 685 с.

8. Юнгер Ф. Г. Совершенство техники. — СПб.: ВЛАДИМИР ДАЛЬ, 2002.- 553 с.

9. Гарт Л. Стратегия. — М., 1956. — 456 с.

10. Глобалізація і безпека розвитку: Монографія / Білорус О. Г., Лук'яненко Д. Г. та ін.; керівник авт. колективу і наук. редак. О. Г. Білорус. — К.: КНЕУ, 2001. — 733 с.

11. Чернов А. Становление глобального информационного общества: проблемы и перспективы//http://www. isn. ru/public/Book. zip.

12. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу. К.: КНТ, 2007. — 260 с.

13. Дзьобань О. П. Інформаційна безпека у проблемному полі соціокультурної реальності: Монографія. — Х. Майдан, 2010. — 260 с.

14. Пилипчук В. Г., Дзьобань О. П. Інформаційне суспільство: філософсько-правовий вимір: монографія. Ужгород: ТОВ «ІВА», 2014, — 282 с.

15. Бейлин М. В. Новые технологические угрозы информационной безопасности личности//Час вибору: виклики інформаційної епохи: колективна монографія/за заг. ред. О. А. Івакіна, Д. В. Яковлева. — Одеса: Видавничій дім «Гельветика», 2016. — 472 с.

16. Фурашев В. Проект Wikileaks та його сутність // Комуфляж № 2. — 2011.

17. Электронный концлагерь: по етапу идет «Ешелон»// «Русский вестник». — 2003. — № 14. — [Електронный ресурс]. — Режим доступа: http://www.x-libri. ru/elib/smi01405/00000001. html.

18. Сулейманов С. Следим строже чем за русскими/ С. Сулейманов [Электронный ресурс]. — Режим доступа: https:// lenta. ru/ articles/2013/06/01/ bigbro/.

19. Пожидаев Е. Инструментарий тотальной слежки и современная система кибершпионажа/ Е. Пожидаев [Электронный ресурс]. — Режим доступа: https:// regnum. ru/ news/1683920 html.

20. Леонов С. Это холодная война? Российским чиновникам запретили пользоваться сервисами Google / С. Леонов [Электронный ресурс]. — Режим доступа: https:// ura. ru/ news/105185439.

21. Ивей Ван. Китайськая модель разрушает гегемонию «общечеловеческих ценностей» [Электронный ресурс]. — Режим доступа: http://inosmi. ru/ world/20130114/204595110.html.

22. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія/Д. В. Дубов. — К.: НІСД, 2014. — 328 с.

23. Современная мировая политика: Прикладной анализ / Отв. Ред. А. Д. Богатуров. — М.: Аспект-Прессс, 2009.- 588 с.

24. Глобалізація і безпека розвитку: Монографія / Білорус О. Г., Лук'яненко Д. Г. та ін.; керівник авт. колективу і наук. редак. О. Г. Білорус. — К.: КНЕУ, 2001. — 733 с.

25. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: доклад Генерального Секретаря ООН [Электронный ресурс]. — Режим доступа: http:// www. un. org. /ru/ documents/ods. asp?m =A/RES /53/70

26. Cyber Storm Securing Cyber Space Режим доступа: http:// www. dhs. gov / cyber-storm-securing-cyber-space.

27. Remarks by the President on securing our nations cyber infrastructure Режим доступа: http:// www. white house. gov/the_press_offise/Remarks-by-the-President-on-Securing-Our-Nations Cyber-Infrastructure.