СУЧАСНА СИСТЕМА МІЖНАРОДНОГО ПРАВА

УДК 341.23

COOPERATION OF STATES IN THE FIELD OF COMBATING CYBER CRIME AND APPROACHES TO SOLVING THE PROBLEM OF CYBER TERRORISM

СПІВРОБІТНИЦТВО ДЕРЖАВ В СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ ТА ПІДХОДИ ДО ВИРІШЕННЯ ПРОБЛЕМИ КІБЕР-ТЕРРОРИЗМА

СОТРУДНИЧЕСТВО ДЕРЖАВ В СФЕРЕ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ И ПОДХОДЫ К РЕШЕНИЮ ПРОБЛЕМЫ КИБЕР-ТЕРРОРИЗМА

Karyna Shakhbazian
Candidate of Legal Sciences, Chief Scientific Researcher, Centre of Intellectual Property Studies and Technology Transfer NAS of Ukraine, E-mail: karina@nas.gov.ua

Карина Шхбазян
Кандидат юридичних наук, старший науковий співробітник, Центр досліджень інтелектуальної власності та трансферу технологій НАН України,E-mail: karina@nas.gov.ua

Карина Шахбазян
кандидат юридических наук, старший научный сотрудник, Центр исследований интеллектуальной собственности и трансфера технологий НАН Украины, E-mail: karina@nas.gov.ua

Abstract. *Currently, society is evolving into information one, which, on the one hand, simplifies the interaction between participants in public relations, and on the other hand, increases the risk of human rights violations, when using information and communication technologies. Changing the structure and scope of information transfer requires both the subjects of social relations, which have a personal interest in ensuring the highest possible level of security of transmitted data, and the state as a whole as a guarantor of the stability of the legal field of public relations. It is obvious that national security largely depends on information security, and in the course of technical progress, this dependence is only growing. Information, acting as an economic and social guarantee of stability of existence and development of society and the state, is the object of close attention and influence of the state. The introduction of e- document management and the creation of interconnected information resources have made information vulnerable to outside interference.*

The choice is made by the individual user of information-and-communication technologies, by civil society as a whole (for example, by opposing or supporting certain state policies in the information sphere) and by public authorities, as they decide on lawmaking and implementation of relevant norms. Each state is constantly balancing between the principles of respect for human and civil rights and freedoms, integration into the international community, the need to ensure economic growth and national security. However, no domestic policy should outweigh the need for international cooperation in the fight against crime, which should be based on the principles of openness, mutual assistance, development of new forms of cooperation. It seems that international

cooperation in the fight against cybercrime should be carried out with the participation of all countries.

The legal basis of the regime of preservation of information in international law includes the following components: basic principles of human rights protection; the procedure for cross-border circulation of information; protection of confidential information; the status of international bodies implementing a unified legal policy in the field of information protection and its implementation.

It seems that international cooperation in the fight against cybercrime must be carried out with the participation of all countries. At the same time, based on a generalized analysis of the legal framework of international, European and national legislation of the EU countries, a certain approach to the implementation of international cooperation in combating cybercrime is proposed: improving the legal framework for international cooperation, harmonized implementation of developed legal norms into national legislation, improving approaches to information exchange.

Key words: *cybersecurity, cybercrime, international cooperation, international information law.*

Анотація. *Нині відбувається еволюція суспільства в інформаційне, що, з одного боку, спрощує взаємодію між учасниками суспільних відносин, а з іншого боку, підвищує ризик порушення прав людини під час використання інформаційно-комунікаційних технологій. Зміна структури та обсягу передачі інформації вимагає як від самих суб'єктів соціальних відносин, які мають особистий інтерес у забезпеченні максимально можливого рівня безпеки даних, що передаються, так і від держави в цілому як від гаранта стабільності правового поля суспільних відносин, забезпечення безпечного поширення інформації. Очевидно, що національна безпека значною мірою залежить від забезпечення інформаційної безпеки, і в ході технічного прогресу ця залежність лише зростає. Інформація, виступаючи в якості економічної та соціальної гарантії стабільності існування та розвитку суспільства та держави, є об'єктом пильної уваги та впливу з боку держави. Введення електронного документообігу та створення взаємопов'язаних інформаційних ресурсів зробили інформацію досить вразливою для втручання ззовні.*

Вибір здійснює як окремий користувач інформаційно-комунікаційних технологій, так і суспільство в цілому (наприклад виступаючи проти чи підтримуючи певну політику держави в інформаційній сфері), та органи публічної влади, як приймають рішення щодо законотворчості та впровадження відповідних норм. Кожна держава постійно балансує між принципами дотримання прав і свобод людини та громадянина, інтеграцією у міжнародне співтовариство, необхідністю забезпечення економічного зростання та національної безпеки. Однак, жодна внутрішня політика не повинна переважати потреби міжнародного співробітництва у боротьбі зі злочинами, яке має будуватися на принципах відкритості, взаємодопомоги, активності у розробці нових форм взаємодії. Як видається, міжнародне співробітництво у боротьбі з кіберзлочинністю необхідно здійснювати на основі участі всіх країн.

Правові основи режиму збереження інформації у міжнародне право включають такі його складові: базові принципи; порядок транскордонного обігу інформації; захист конфіденційної інформації; статус міжнародних органів, що здійснюють вироблення єдиної правової політики у сфері захисту інформації та її реалізацію. Виходячи з узагальненого аналізу нормативно-правової бази як міжнародного, європейського та національного законодавства країн ЄС, пропонується певний підхід до реалізації міжнародного співробітництва у сфері боротьби з кіберзлочинами, що передбачає скоординованість дій усіх держав таким напрямам як удосконалення правової основи взаємодії та імплементація вироблених норм у національне законодавство, покращення підходів до обміну інформацією.

Ключові слова: *кібербезпека, кіберпреступність міжнародна співпраця, міжнародне інформаційне право.*

Аннотация. В настоящее время происходит эволюция общества в информационное, что, с одной стороны, упрощает взаимодействие между участниками общественных отношений, а с другой стороны, повышает риск нарушения прав человека при использовании информационно-коммуникационных технологий. Изменение структуры и объема передачи информации требует как от самих субъектов социальных отношений, имеющих личный интерес в обеспечении максимально возможного уровня безопасности передаваемых данных, так и от государства в целом как от гаранта стабильности правового поля общественных отношений, обеспечения безопасного распространения информации. Очевидно, что национальная безопасность в значительной степени зависит от обеспечения информационной безопасности и в ходе технического прогресса эта зависимость только растет. Информация, выступая в качестве экономической и социальной гарантии стабильности существования и развития общества и государства, является объектом пристального внимания и влияния государства. Введение электронного документооборота и создание взаимосвязанных информационных ресурсов сделали информацию достаточно уязвимой для вмешательства извне.

Выбор осуществляет как отдельный пользователь информационно-коммуникационных технологий, так и общество в целом (например, выступая против или поддерживая определенную политику государства в информационной сфере), и органы публичной власти, как принимают решения о законотворчестве и внедрении соответствующих норм. Каждое государство постоянно балансирует между принципами соблюдения прав и свобод человека и гражданина, интеграцией в международное сообщество, необходимостью обеспечения экономического роста и безопасности. Однако ни одна внутренняя политика не должна преобладать над необходимостью международного сотрудничества в борьбе с преступлениями, которое должно строиться на принципах открытости, взаимопомощи, активности в разработке новых форм взаимодействия. Как представляется, международное сотрудничество по борьбе с киберпреступностью необходимо осуществлять на основе участия всех стран.

Правовые основы режима хранения информации в международном праве включают следующие его составляющие: базовые принципы; порядок трансграничного обращения информации; защита конфиденциальной информации; статус международных органов, осуществляющих выработку единой правовой политики в сфере защиты информации и ее реализации. Исходя из обобщенного анализа нормативно-правовой базы как международного, европейского, так и национального законодательства стран ЕС, предлагается определенный подход к реализации международного сотрудничества в сфере борьбы с киберпреступлениями, предусматривающий скоординированность действий всех государств по таким направлениям как усовершенствование правовой основы взаимодействия, гармонизированная имплементация выработанных норм в национальное законодательство, улучшение подходов к обмену информацией.

Ключевые слова: *кибербезопасность, киберпреступность, международное сотрудничество, международное информационное право.*

Introduction. Currently, society is evolving into information one, which, on the one hand, simplifies the interaction between participants in public relations, and on the other hand, increases the risk of human rights violations, when using information and communication technologies. Changing the structure and scope of information transfer requires both the subjects of social relations, which have a personal interest in ensuring the highest possible level of security of transmitted data, and the state as a whole as a guarantor of the stability of the legal field of public relations. It is obvious that national security largely depends on information security, and in the course of technical progress, this dependence is only growing. Information, acting as an economic and social guarantee of stability of existence and development of society and the state, is the object of close attention and influence of the state. The introduction of e- document management and the

creation of interconnected information resources have made information vulnerable to outside interference.

The purpose of research. The purpose of this article is, based on a generalized analysis of the legal framework of international, European and national legislation of the EU countries, to propose a certain approach to the implementation of international cooperation in combating cybercrime.

Literature review. In recent years, Ukrainian scientists in the sphere of IT technologies, sociology, economy, and law have been paying significant attention to the issue of cybersecurity. Mostly, the issue of cybersecurity is studied from the point of view of computer sciences (applied aspect): Furashev V., (2012), in legal sciences much attention is paid to national regulation of this issue in Ukraine: the theoretical basis of cyber-relations (Gnatiuk S., 2013), information, and cyber-security (subject, object, relations, etc.): works of Lipkan V., (2017), Sopilko I.,(2016), Dovgan O., (2018) studying of provisions of Ukrainian law in the sphere of information and security, cybersecurity from point of view of criminal law and administrative law (i.e. Doronin I., 2017; Diorditsa I., 2017), cybersecurity as a strategy of national information law order (i.e. Tkachuk N., 2019; Gutsaliuk M., 2019; Halinska K., 2016), etc.

Research results. At present, the postindustrial society is being transformed into an information society, which, on the one hand, simplifies the interaction between participants in public relations, and, on the other hand, increases the risk of violating confidentiality. Changing the structure and volume of information transferred requires both the subjects of social relations, who have a personal interest in ensuring the highest possible level of security of the transmitted data, and the state, as a guarantor of the public relations stability, to build clear architecture for the safe dissemination of information.

Obviously, national security depends to a large extent on ensuring information security, and this dependence only grows in the course of technological progress. Information, acting as an economic and social guarantee of the stability of the existence and development of society and the state, is the object of close attention and influence of the state authorities. The introduction of full-fledged electronic document circulation and the creation of interoperable information resources made information matter sufficiently vulnerable to outside interference. The legal basis of the regime of confidentiality of information in international law includes the following components: basic principles in the field of privacy; the procedure for cross-border turnover of confidential information; protection of confidential information; the status of international bodies engaged in the development of a unified legal policy in the field of privacy and its implementation. Based on a generalized analysis of the regulatory framework of both international and national legislation and current views on this problem, the new approach towards the implementation of international cooperation in the field of combating cybercrime can be proposed. Such an approach should imply greater coordination of actions of all states, at least in two directions: improving the legal basis for interaction and implementation of the developed norms into national legislation, completing the organizational basis for the exchange of information.

Each state is constantly balancing between the principles of observance of rights and freedoms of a person and a citizen, integration into the international community, and from another side - the need to ensure economic growth and national security, including restrictions of human and civil rights and freedoms, the establishment of restrictions on entrepreneurial activity, protection of its own interests in the international arena.

It appears that international cooperation in the fight against cybercrime needs to be implemented based on the participation of all countries, which is predetermined both by the property of the information itself as an object of encroachment and by the nature of committed crimes. As noted by the international expert on harmonization of legislation in the field of cybercrime, Stein Schjolberg, “cyberspace, as the fifth common space, after terrestrial, sea, air and space, requires coordination, cooperation and special legal measures at the international level” [Schjolberg S., 2010].

In the modern world, information is the most important component of the development of society. The transformation of a postindustrial society into an information society means that information becomes global, becomes significant both for a person and for the state and society as a whole, everyone can seek, receive, transmit, produce and disseminate information by any legal way, there are no boundaries for its flow. At the moment information is recognized as one of the most important values, accordingly, its protection is no less important activity than its receipt and transmission, therefore, in a "digitalized society at the beginning of the 21st-century sphere of risk is changing" [Sindhu K.K., Kombade R., 2012]. The widespread use of information processing facilities by computers with software that makes it relatively easy to modify, copy and destroy information increases the vulnerability of the information space.

It is very important to understand the global nature of the cybercrime problem. So, already now, cyberattacks paralyze the work of not only private structures, but also state bodies, in the world, there is no state that is enough protected from this kind of attack. As potential sources of cyber threats, are considered not as such not only hackers or their groups, but also whole states, terrorist and criminal groups.

Symantec Security, global cyber security service, says "every second 12 people are being cyberattacked around the world, and annually in the world, there are about 556 million cybercrimes, the damage from which is more than $ 100 billion".

Cybercrime can violate the interests of both the state and the individual. Undoubtedly, the features of the functioning of information systems, primarily the Internet, "require that the solution cybersecurity issues were addressed joint efforts of various actors - public and private" [Huey L., 2013], however, it is the state that is only capable of effectively carrying out a full-scale counteraction committing cybercrimes.

There are examples in the world of fairly effective systems for countering cybercrimes. Currently, leading countries of the world are actively expanding and creating in the armed forces and special services the units, which should ensure the development of offensive capabilities in cyberspace.

For example, in the USA, along with the already functioning National Cyber Security Center, as part of The Armed Forces has been formed the Unified Cyber Command (Unified U.S. Cyber Command), which in a global scale should coordinate the efforts of all structures of the Pentagon during the conduct of military actions, provide appropriate support civil federal institutions, and also interact with similar departments of other countries. At the same time, these organizations are partly controlled departments, since the supreme controlling structure is the National Security Council with special committees, whose area of responsibility includes the implementation of an information strategy, including the fight against cybercrime. In the UK cyberweapon programs are implemented - they will ensure the ability of the authorities to withstand the growing threats from cyberspace. Australia has established an Email Security Coordination Group (ESCG). The main task of this group is to create a secure and reliable electronic operational space for both the public and private sectors. Cybercrime countermeasures are not limited to the activity of individual states, but also their blocs, in particular NATO. The strategic NATO concept for the first time included a provision on cyberspace as a new area of the military activities of the alliance.

In other words, in the fight against cross-border crimes, which include a significant part of cybercrimes, a special role is assigned to states: only when there is well-coordinated work of law enforcement agencies of different countries, then it becomes possible to reduce the number of offenses committed in this area.

International cooperation is carried out in several directions and presupposes, first of all, the creation of regulations and the development of general recommendations, as well as the introduction of effective models of organizational interaction between states.

Legal regulation of issues of struggle against cybercrime is the basis of the entire system of countering cybercrime. The complexity of the development of international instruments is further

complicated by the fact that existing laws are difficult to apply when it comes to not localizable attacks on a planetary scale, the evidence of which is scattered and virtual.

The international community in various levels has developed a number of acts that are significant for the fight against cybercrime, with a special role played by regional acts, since the worldwide document is currently quite difficult to elaborate.

At the same time one can note the attempts of states to spread the norms of global international treaties on cybercrime issues or attempts to conclude new treaties. For example, so both in cyberspace along with individual persons organized criminal groups can act, there is a possibility of application of international treaties aimed at combating organized crime to them - in particular, the UN Convention against transnational organized crime of November 15, 2000. In addition, the concept of the UN Convention on ensuring international information security [UN Convention, 2000], presented to the international community in November 2011 at the Conference on Cyberspace in London; it includes a preamble, 23 articles combined into the main part, and final provisions.

It is important that in Art. 4 of the aforesaid Convention there are stipulated main threats to the international peace and security in the information space, of which 11 ones are basic and 4 – are additional. Basic ones include: 1) the use of information technology and means of storing and transferring information to engage in hostile activity and acts of aggression; 2) purposefully destructive behavior in the information space aimed against critically important structures of the government of another State; 3) the illegal use of the information resources of another government without the permission of that government, in the information space where those resources are located; 4) actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilizing society; 5) the use of the international information space by governmental and non-governmental structures, organizations, groups, and individuals for terrorist, extremist, or other criminal purposes; 6) the dissemination of information across national borders, in a manner counter to the principles and norms of international law, as well as the national legislation of the government involved; 7) the use of an information infrastructure to disseminate information intended to inflame national, ethnic, or religious conflict, racist and xenophobic written materials, images or any other type of presenting ideas or theories that promote, enable, or incite hatred, discrimination, or violence against any individual or group, if the supporting reasons are based on race, skin color, national or ethnic origin, or religion; 8) the manipulation of the flow of information in the information space of other governments, disinformation or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society, or eroding traditional cultural, moral, ethical, and aesthetic values; 9) the use, carried out in the information space, of information and communication technology and means to the detriment of fundamental human rights and freedoms; 10) the denial of access to new information and communication technologies, the creation of a state of technological dependence in the sphere of informatization, to the detriment of another State; 11) information expansion, gaining control over the national information resources of another State.

Additional factors, increasing the danger of the aforementioned threats, are: 1) difficulty in identifying the source of hostile actions, especially taking into account the growing activity of individuals, groups, and organizations, including criminal organizations, which provide intermediary services, carrying out activities in the name of others; 2) the potential danger of the inclusion of undeclared destructive capabilities in information and communication technology; 3) the difference in the levels of information and communication technologies in use, and in their security, in different States ("digital inequality"); 4) the difference in national legislation and practices as regards the formation of a secure and quickly restorable information infrastructure.

However, again we have to admit that in the concept the principles of the draft convention there is not spelled out in detail plan of international cooperation in the fight against cybercrimes, except for actions against terrorists. The inclusion into the concept of the Convention Ch. 5 “International cooperation in the field of international information security " is a positive sign, but

measures of international cooperation in this area seem to be clearly insufficient for the effective functioning of the system of international security since they only assume “exchange best practices on the prevention, legal investigation, and the liquidation of consequences of crimes, including those related to terrorism, involving the information space", “consultations on the issues of activities in the information space, which can cause the concern of the participating States, and cooperation regarding the settlement conflict situations of a military nature ". At the same time, these forms do not take into account the need for operational interaction of law enforcement bodies on a wide range of issues.

Thus, the provisions of the concept of the UN Convention on the provision of international information security are of a sufficiently compromise nature and are oriented primarily to prevent information wars and terrorism.

It should be noted, that majority of the specialized acts for the fight against cybercrimes constitute acts of the European Union, which has one of the most developed in the world information security systems. So, in October 1999 during the Tampere Meeting of the European Council, it was decided on the advisability of including crimes in the field of high technologies (*high-tech crime*) among crimes for which it is necessary to develop a common European approach in terms of criminalization and sanctions. In 2001, the European Commission submitted a special Message “Creating a secure information society through increasing the security of information infrastructure and combating crime with using computer tools" [Communication, 2001], which contained proposals for legal and organizational nature to combat cybercrime in the European Union.

The Budapest Convention on Cybercrime is of fundamental importance both for the European Union and for the entire world community, governing global control measures with cybercrime, which was adopted by the Council of Europe in 2001 [Convention on Cybercrime, 2001].

In the preamble to the Convention, the States – Parties outlined the purpose of its adoption: the development, as a priority, of a common policy in the field of criminal law, focused on protecting society from cybercrime, including through appropriate legislative acts and strengthening of international cooperation; deterring actions against the confidentiality, integrity, and availability of computer systems and networks and computer information, as well as against abuse of such systems, networks, and information, by ensuring that such acts are criminalized and granting powers sufficient to the effective fight against these crimes by helping to identify and by the investigation and prosecution of such criminal offenses, both domestically and internationally and by developing agreements on operational and reliable international cooperation.

The Cybercrime Convention calls for action to be taken by the participating States and at the international level. At the national level, the development of primarily material criminal law to be taken: development in national criminal codes norms on offenses against confidentiality, integrity and availability of computer systems, crimes, related to networks and information, related to the use of computer tools, data content, in violation of copyright and related right; establishment of criminal liability of legal entities, which, however, contradicts the concepts of criminal responsibility in a number of countries.

Thus, in the Convention on Cybercrime, cybercrimes are classified as follows: 1) offenses against the confidentiality, integrity, and availability of computer data and systems: illegal access; illegal interception; data interference; system interference; misuse of devices; 2) computer-related offenses: computer-related forgery; computer-related fraud; 3) content-related offenses - offenses related to child pornography; 4) offenses related to infringements of copyright and related rights.

Additional Protocol to the Convention on cybercrime includes a list of the following types of crimes: 1) dissemination of racist and xenophobic material through computer systems; 2) racist and xenophobic motivated threat; 3) racist and xenophobic motivated insult; 4) denial, gross minimization, approval or justification of genocide or crimes against humanity). [Additional Protocol, 2003]

The Convention also presupposes the development of criminal procedure legislation, for example, the need to legally secure the operational security of accumulated computer data, the procedure for conducting a search and seizure of stored computer data. The Convention focuses on international cooperation (chapter 3).

The general principles of international cooperation are: general principles of mutual assistance; the possibility of cross-border access to stored computer data from the corresponding consent or to publicly available data, mutual assistance in connection with the evaluation of stored electronic data, mutual legal assistance to collect data on streams in real-time; network creation 24/7). Despite the presence in the considered sphere of other international acts, The Convention is the only recognized international treaty, containing the norms of material and procedural rights to counter cybercrime and protect freedom, security and human rights on the Internet. The provisions of the Convention provide the basis for the interaction of states, however, as noted by the Bulgarian researcher R. Georgieva, "The Convention does not guarantee the safety of the virtual space. Of great importance, it will be to have its coordination with the domestic legislation of each country" [Georgieva R., 2001].

Within the framework of the European Union, a number of programs that contribute to the fight against cybercrime, are being developed. In particular, the Stokholm Program recommends preparing an internal security strategy for the EU to improve the protection of citizens and to combat organized crime and terrorism. At the regional level, in addition to the Convention on Cybercrime, the Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Sphere of Computer Information was adopted of June 1, 2001. Basic idea of these documents is the definition of uniform compositions of computer crimes that states must include in their national legislation, as well as the development of measures to combat them. The treaties under consideration fulfill a very important role: they establish the foundations of the jurisdiction of states in criminal matters on the Internet and the rules of international cooperation, ensuring the consistency of the states in the fight against computer crimes.

In general, these treaties provide for a system of interrelated international and national measures to combat computer crimes. It is important to note, that the interaction of states in the fight against cybercrimes requires a generalization of the legal norms of various states when regulating the actions of the parties in the process of such struggle. In particular, the NATO Center of Best Practices in Computer Security published the "Tallinn Manual on the International Law Applicable to Cyber Warfare". The main tasks are supposed to "adapt the existing legal norms in relation to armed conflicts under the specifics of hostile activity in the virtual space", and an attempt to develop definitions of basic concepts in the field of computer security [Tallin Manual, 2012].

The second form of cooperation between states in the fight against cybercrime is the creation of specialized bodies. Because an information security state is associated with its sovereignty, then the creation of a single body that would coordinate the interaction of states to combat cybercrime, is difficult, however, subsidiary bodies are created, guided by uniform performance standards, generalizing the practice of different countries on issues of combating cybercrimes. Of great importance in the interaction of the states - members of the European Union is the activity of Europol and Eurojust, which are directly involved in the fight against cybercrime in the European Union.

Eurojust carries out coordination of law enforcement bodies of various states on the investigation of cybercrimes, assists in the investigation on the request of the relevant public authority of the member states of the European Union, provides law enforcement agencies from these countries information on ongoing investigations on cybercriminals [Eurojust casework in 2015, 2016].

Eurojust's mandate also extends to initiating criminal investigations or putting forward a proposal to initiate an investigation to the law enforcement authorities of the EU member states and

subsequent coordination of ongoing investigations. In addition to these bodies, possessing jurisdictional competence in this area, the European Union creates also subsidiary bodies.

Also, on January 18, 2013, European Center on Combatting Cybercrime was officially opened in the Hague. Its goals are the creation of the data collection and processing of data on cybercrimes, the expertise of Internet threat assessments, development and implementation of advanced methods of prevention and investigation of cybercrimes, preparation of new personnel, assistance to law enforcement and the judiciary, as well as coordination of joint actions of stakeholders, aimed at improving the level of security in European cyberspace.

The military interaction of states also requires a solution to the issue of their cooperation in the field of organizational support for the struggle against cybercrime. Thus, in 2008, at the initiative of Estonia, a Center of NATO Best Practices was established in Tallinn, acting as a research and educational center and dealing with the development of key directions of coalition capabilities in cyberspace. Also, in 2013, NATO completed its unified cyber threat response system, which includes two Cyber Threat Response Centers (Brussels and Mons). Besides, steps are being taken to test the effectiveness of the already established cyber-attack mitigation system, for example, there are trainings been annually held: "Cybercoalition", "Shield ball".

In other words, the current trend of international counteraction to cybercrime is the expansion of the sphere of the interaction of states. Such methods as operational cooperation of law enforcement agencies in the fight against cybercrime (Interpol, Europol, Eurojust), creation and use of a unified database on cybercriminals, committed and planned cybercrimes (primarily working in 24/7 mode) turned into reality.

Insofar as the introduction of normative acts of both national and international character is an insufficient step towards solving the problem of combating cybercrime, in this case, we need special knowledge in the field of information technology and software. A single global act governing the procedure for countering cybercrimes has not been developed, but the international community within the framework of the regional cooperation takes measures to regulate legislatively the actions of subjects in cyberspace, to combat cybercrime.

If we speak about legal features of countering cyberterrorism in foreign law in the context of the development of the modern information space, it was noted that such principles of IT technologies as openness and general accessibility are widely used by terrorist organizations for their criminal purposes.

An analysis of foreign legislation suggests that in most countries of the world there is no special corpus delicti - cyber terrorism. At the same time, the reference to the use of IT technologies in the spread of ideas of terrorism is fixed as an aggravating circumstance. One can come to the conclusion, that there is no consensus in legal doctrine regarding including cyber-terrorism into criminal law at national level. Two types of cyber-terrorism can be determined, proceeding from types of actions taken: hybrid and pure one. In the first case, it is the use of the Internet for terrorist activities: propaganda, recruiting supporters, training them, radicalizing society, collecting funds, obtaining data, communicating, planning real terrorist attacks. In the second case, these are direct attacks on cyberinfrastructure in order to achieve political, religious and ideological goals.

More and more industrial facilities are operated from remote computers, more and more information bases are systematized thanks to cloud programs. Simultaneously, the global network allows you to get easy access to a large audience in the absence of censorship, thanks to which the dissemination of information takes on qualitatively different forms. It is believed that Barry Collin (an employee of the Institute for Security and Intelligence, California, USA) back in 1980, when only several computers of the U.S. Department of Defense have been linked together through a network ARPANET was the first researcher who for the first time mentioned “cyberterrorism” [B. Collin, 1996]. Among the first attempts to use the Internet for illegal purposes were actions, made by the group “Tamil Tigers”, which in 1998 “bombed” with electronic letters the official institutions of Sri Lanka, calling themselves "black Internet tigers" in them. Around the same time, sect “Aum Shinrikyo” (the data was obtained during searches at the headquarters of the organization) was developing the possibility of intercepting control of nuclear facilities.

For the first time about “digital Pearl Harbor "was written in 1995 [J. Lewis, 2003]. America seemed a defenseless victim even facing the most insignificant computer actions [Weimann G., 2005]. “Such a whipping up of hysteria had been going on for ten years, right up to the time when G. Weimann in 2004 designed it step by step in the near future” [Weimann G., 2004].

Analysis of foreign criminal legislation also shows reluctance to introduce cyber terrorism into national legal systems, which should not be considered as a kind of "conspiracy of silence". In some countries, there is only mention of the use of telecommunication systems in terrorist purposes, which in most cases can be considered as an additional aggravating circumstance.

For example, Art. 421-1 Criminal Code of France, providing for the concept of an act of terrorism, only complements that it will also apply to criminal acts in the field of informatics in case of identifying their target focus. Herewith reference is made to Book III of the Criminal Code, establishing criminal liability for crimes in the sphere of computer information. After the appearance of special electronic journals and sites promoting terrorist actions, Art. 421-2-5-2, which introduced criminal liability for distribution of messages on the Internet, images, other informational actions, including the display of deliberate attacks for life with a demonstration of commitment to terrorist ideology was included.

Italian criminal legislation has its own specifics. So, in addition to special acts of terrorism in the Criminal Code of Italy, there is a general rule (Art. 280), which makes it possible to refer to terrorists practically any offense provided for by the Code, if it is was committed for that purpose. Attention to cyber terrorism in Italy can be traced to Art. 270-quinquies of its Criminal Code, establishing responsibility for terrorist training. In 2005 this article was introduced in the Criminal Code of Italy, but in 2015 received an important addition - the punishment increases when teaching with the use of IT technologies.

Thus, in some foreign countries, we can see attempts to apply measures of criminal law enforcement with the aim of countering cyber-terrorism, however, it seems that in its current form, this kind of regulation speaks rather about the problem statement than about its possible decision.

Much skepticism about the very phenomenon - cyber terrorism - is present in the United States and Western Europe. Many researchers point out that at the moment there are no reliable data on the real possibilities of terrorist organizations infiltrating into remote control systems and damaging critically important infrastructure facilities.

In the scientific literature, there are references to annual USA national intelligence reports, containing the assessment of cybersecurity of the country. For example, in the introductory part Dennis Blair's 2010 report there is present an overall assessment of cybersecurity, highlighting the prospects for the development of cybercrime. Only a passing mention is made of the ability of criminals to interfere with remote access to critical facilities and infrastructure. At the same time, forms of countering cyber terrorism are associated with the concept of "America's enemy" without deciphering it. Further, where the basic characteristics of threats are given on the part of the main terrorist organizations, there is no mention of the cyber capabilities of criminals. However, in relation to Al-Qaeda there is made the remark about its preparation a large-scale action against the United States in order to inflict the greatest damage to the country's economy [D. Blair, 2010].

To a large extent, public opinion about the significance of the cyber terrorism threat in the United States is formed by the reports of the country's national intelligence service.

In 2011, James Clapper, Head of the Service, does not mention cyber terrorism as a threat at all, presenting a general outline of the development of crimes in the field of computer information. [Statement for the Record on the Worldwide Threat Assessment, 2011]

In 2012, the Head of National Intelligence points to the global spread of smartphones and the development of cloud technologies for organizing information as a risk factor. But even in this case, the term "cyber terrorism" is not used.[Statement on global Security, 2012] The close interaction of state authorities and the private sector in the field of computer information are indicated as an effective preventive measure.

A 2014 report ranked cyberspace as the number one global threat and identified Russia as a country of concern for US cyber policy and network security [Statement on Global Security, 2014] The report clearly identifies this factor as a threat to America's interests and values.

In the 2017 report, Russia is already identified as the main threat to the US cybersecurity. The main focus is on accusing Russia of influencing the 2016 elections (it is emphasized that such actions could be carried out only with the consent of senior officials). Russian hackers are said to have carried out "devastating" cyberattacks on critical US infrastructure [Statement on Global Security, 2017]. Such forecasts are made with the aim of forming a certain public opinion for the subsequent substantiation of additional restrictions imposed on Internet communication, the introduction of special forms of regulation of communication technologies, and the expansion of the powers of national special services.

R. Knake in 2017, presenting recommendations to the Trump administration, explicitly advises considering cyberattacks as "an armed attack entailing a military response" [R. Knake, 2017]

Expert of Council on Foreign Relations, Robert Knake, cites the following statistics: out of more than 63 thousand cases of terrorism in 2000–2010 yy, none are associated with cyber terrorism. Al-Qaeda has never been able to carry out cyberattacks to US facilities that could lead even to minor damage [R. Knake, 2010]. By the way, R. Knake in his expert assessments always speaks with restraint about cyber terrorism. Already in 2015 this expert supported international efforts on the prevention of computer crime, welcoming proposals to introduce compulsory national responsibility states from whose territory were committed malicious cyberattacks [R. Knake, 2015]. The state should form a national legal framework so that internet service providers were required to monitor malicious traffic and close access to it. However, at the same time, he indicated that the proposal should be supported primarily by the United States.

The definition of cyber terrorism, presented by foreign experts in 2017 for Tunisia [M. Zerzri, 2017], looks interesting with the aim of applying it in the activities of state authorities and the country's special services. It highlights the following features:

- –is performed through cyberspace by individuals, groups or organizations directly influenced by terrorist movements and / or their leaders;
- motivated by a desire to bring about political or ideological changes;
- causes violence, due to which the physical and psychological consequences can go far beyond the immediate victim or the target of the impact.

At the same time, cyber terrorism is classified into hybrid and pure cyber terrorism. In the first case, this is the use of the Internet for terrorist activities: propaganda, recruiting supporters, training them, radicalizing society, collecting funds, obtaining data, communicating, planning real terrorist attacks, in the second, direct attacks on cyberinfrastructure to achieve political, religious and ideological goals.

Cyber terrorism in its pure form is divided into destructive and subversive. Disruptive cyber terrorism is the destruction of information system functions to damage or destroy virtual and physical assets. The most popular way is the use of computer viruses, worms, Trojans, and extortion. Subversive cyberterrorism means hacking into computer networks that provide critical infrastructure (medical care, transport, financial systems, etc.) that disrupts the normal life of society, the state, and citizens. Attention is drawn to the fact that at present, hybrid cyberterrorism, associated with the propaganda of terrorist ideas, training supporters, recruiting them, and preparing them to carry out single attacks, is becoming the most widespread. The Internet, due to its openness, also influences the structure of terrorist organizations, which are increasingly turning into a networked community that does not have centralized control.

Hybrid cyber terrorism associated with the propaganda of terrorist ideas has the most direct impact on the mass consciousness of citizens. In terms of the strength of the psychological impact, the effect of it often significantly exceeds the consequences of a direct terrorist attack [M. Gross, 2016]. In the context of the instability of the socio-political situation around the world, terrorist organizations have realized that thanks to pinpoint impacts that do not require significant financial

costs and in-depth knowledge of computer systems, it is possible to achieve very far-reaching results.

Conclusions

The importance of cybersecurity issues at the international level is confirmed by the fact that with few exceptions (most notably, the Budapest Convention on Cybercrime and the not-yet-in-force African Union Convention on Cyber Security and Personal Data Protection), international law does not regulate cyberspace, leaving this task for. national authorities or international expert groups.

Insofar as the introduction of normative acts of both national and international character is an insufficient step towards solving the problem of combating cybercrime, in this case, we need special knowledge in the field of information technology and software. A single global act governing the procedure for countering cybercrimes has not been developed, but the international community within the framework of the regional cooperation takes measures to regulate legislatively the actions of subjects in cyberspace, to combat cybercrime. The current trend of international counteraction to cybercrime is the expansion of the sphere of the interaction of states. Operational cooperation of law enforcement agencies in the fight against cybercrime (*Interpol, Europol, Eurojust*) turned into reality as well as creation and use of a unified database on cybercriminals, committed and planned cybercrimes.

The international law of cybersecurity is just over 20 years old, it remains in a state of formation. The great problem remains, relating to the issue of state sovereignty in cyberspace. The absence of a unified international legal basis has led to the fact, that many States are conflicted over the application and interpretation of key aspects of international law in the cyber context, relating to volume and borders of rights and obligations of cyberspace users (of all types – including those who create content and those who consume it, as well as content- and internet services- providers). Speaking of cyberterrorism and cybercrime leads us to the issue of limitation of our human and civil rights, which can be applied to us in the face of protection of national security. International law can become the only system of supports and counterbalances between human rights protection in cyberspace and firewall against hostile cyber operations at the international level.

The fight against cybercrime (and therefore also against cyberterrorism) will have a meaningful impact only when the efforts of the entire international community to be united. The criminalization of such actions in one country can be easily circumvented by the lack of accountability in another. As a possible solution, one can propose to introduce a universal jurisdiction in which the attacked state can demand investigation, punishment of the perpetrators, and compensation for damage from the state from the territory of which the attack was carried out.

Thus, the legal framework for countering cybercrime and, particularly, cyberterrorism through the prism of the socio-political dimension is based on the following general points:

1. Cyberterrorism is now a slightly exaggerated threat. Standard cybercrime causes more significant damage to the economy of any state, taking into account that cybercrime is extremely widespread.

2. All over the world there are certain discrepancies in the understanding of cyber terrorism. Experts admit that it is often impossible to draw a line between this phenomenon and the manifestation of ordinary cyber criminality. Traditionally, there is a broad understanding of cyber terrorism (any use of computer networks for terrorist purposes) and a narrow one (actions aimed at causing specific damage to infrastructure, life and health of citizens).

3. The analysis showed that, despite the applicability of the principles and norms of modern international law to the information sphere, universalization of the existing international legal regulation in relation to cyberspace is required, taking into account its specifics and in order to counter effectively the use of information and communication technologies for illegal purposes. The efforts of states to develop special rules of conduct in cyberspace are currently focused on a narrow sphere of issues related to human rights, data privacy, etc. Not all states are interested in creating a modern and effective mechanism for cooperation in cyberspace, openly opposing the development

of new international legal instruments, which entails the lack of a full-fledged universal international legal framework for cooperation in the field of cyberspace.

4. Based on the conducted analysis of doctrine and practice, the conclusion can be made about the need to create a universal international legal framework for cooperation in the field of cyberspace. In modern international law, cybersecurity is one of the most pressing problems directly related to the security of the state. The difference in the approaches of states to the problem of ensuring cybersecurity at the present stage entails the absence of an effective multilateral legal framework for cooperation in this area.

References

1. Additional Protocol to the Convention on Cybercrimes concerning the criminalization of acts of a racist and xenophobic nature, carried out by means of computer systems (signed in Strasbourg on 28 January 2003). <http://mvd.gov.by/main.aspx?Guid = 4593> [20.11.2021]

2. Blair D. Annual Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence / D. Blair. — USA : National Intelligence, 2010. <https://www.dni.gov/files/documents/Newsroom/Testimonies/20100203_testimony.pdf.> [20.11.2021]

3. Collin B. The Future of CyberTerrorism / B. Collin // XI Annual International Symposium on Criminal Justice Issues. — Chicago: Univ. of Illinois, 1996. — P. 285–289.

4. Communication from the Commission to the Council the European Parliament, the Economic and Social Committee and the Committee of the Regions "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime". Brussels, 26 January 2001. COM (2000) 890fi nal. <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/ Crime / CrimeCommEN.html> [20.11.2021]

5. Convention on ensuring international information security (concept). <http://www.scrf.gov.ru/documents/6/112.html> [20.11.2021]

6. Eurojust fights serious, cross-border organized crime // Eurojust casework in 2015 (Eurojust infographics). <http://www.eurojust.europa.eu/press/PressReleas es / Pages / 2016 / 2016-03-04.aspx>[20.11.2021]

7. European Convention on Cybercrimes (Crimes in Cyberspace): concluded in Budapest on 23 Nov. 2001 <http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm> [20.11.2021]

8. Forensic Investigation Processes for Cyber Crime and Cyber Space / K.K. Sindhu, R. Kombade, R. Gadge, B.B. Meshram // Proceedings of International Conference on Internet Computing and Information Communications. — 2012. — Vol. 16. — P. 193–206.

9. Gross M.L. The Psychological Effects of Cyber Terrorism / M.L. Gross, D. Canetti, D.R. Vashdi // Bulletin of the Atomic Scientists. — 2016. — Vol. 72, iss. 5. — P. 284–291.

10. Huey L. Uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime / L. Huey, J. Nhan, R. Broll // Criminology and Criminal Justice. — 2013. — Vol. 13, № 1. — P. 81–97.

11. Knake R.K. Cyberterrorism Hype v. Fact / R.K. Knake // Council on Foreign Relations. — 2010. — 12 Febr. <https://www.cfr.org/expert-brief/cyberterrorism-hype-v-fact> [20.11.2021]

12. Knake R.K. Cleaning Up U.S. Cyberspace / R.K. Knake // Council on Foreign Relations. — 2015. — Dec. https://cfrd8-files.cfr.org/sites/default/files/pdf/2015/12/Cleaning_Up_CyberBrief.pdf [20.11.2021]

13. Knake R.K. A Cyberattack on the U.S. Power Grid: Contingency Planning Memorandum No. 31 / R.K. Knake // Council on Foreign Relations. — 2017. — Apr. https://cfrd8-files.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf [20.11.2021]

14. Lewis J. Cyber Terror: Missing in Action. Knowledge, Technology & Policy, 2003, vol. 16, iss. 2, pp. 34–41.

15. Schjolberg S. A cyberspace treaty — A United Nations convention or protocol on cybersecurity and cybercrime [Electronic resource] / Stein Schjolberg // Twelfth United Nations

Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010. <http://cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf> [20.11.2021]
16. Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence, 2010. <http://www.au.af.mil/au/awc/awcgate/dni/threat_assessment_10feb11.pdf.> [20.11.2021]
17. Statement for the Record Worldwide Threat Assessment of the US Intelligence Community House Permanent Select Committee on Intelligence, 2014. <https:// www.globalsecurity.org/intell/library/congress/2014_ hr/140204-clapper.pdf>. [20.11.2021]
18. Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence, 2017. < https://www. intelligence.senate.gov/sites/default/files/documents/oscoats-051117.pdf> [20.11.2021]
19. Tallinn Manual on the International Law Applicable to Cyber Warfare. <https://icdt.osu.edu/tallinn-manual-international-law-applicable-cyber-warfare> [20.11.2021]
20. Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence, 2012. <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/hpscifinalunclasssfrfeb 022012).pdf>. [20.11.2021]
21. Weimann G. Cyberterrorism: The Sum of All Fears? / G. Weimann // Studies in Conflict & Terrorism. — 2005. — № 28. — P. 129–149.
22. Weimann G. Cyberterrorism: How Real Is the Threat? / G. Weimann. <https://www.usip.org/sites/default/files/sr119.pdf> [20.11.2021]
23. Zerzri M. The Threat of Cyber Terrorism and Recommendations for Countermeasures / M. Zerzri // Center for Applied Policy Research. — 2017. — № 4. — < https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf.> [12.11.2021]
24. R. Georgieva (2001) Георгиева Р. Конвенция за киберпрестъпността / Р. Георгиева // Общество и право (София). — 2001. — № 11. — С. 16–18.