The intensive development and widespread dissemination of information and communication technologies (hereinafter referred to as ICT) in the modern world in the focus of the complication of social relations in the direction of political and economic unification and diversification determines the modernization of society, which manifests itself in the digitalization of social relations and management processes, as well as in the creation of on the basis of the Internet network of an integrated information space. At the same time, the globalization of the economy, accompanied by an exponential growth in the introduction of new telecommunication technologies and an active digital transformation of various spheres of society (for example, communications, transport, state and municipal administration, defense, medicine, education, energy, financial system, and national security), increasingly predetermines the spread of terrorist acts using high technologies in the information space. In this context, such destructive use of ICT in order to undermine public order, destabilize the work of government bodies and weaken the country’s economic system, such as cyberterrorism, draws special attention to itself.

Academic interest in cyberterrorism is dictated by the special nature of the public threat of terrorism in general, which is expressed in infringement on state security, public order, and civil peace. In the specialized literature, particular attention is also paid to increasing of the information and technological potential of terrorist organizations (http://www.consultant.ru), which predetermines new threats to the economic stability of individual states, which can cause enormous material damage (both direct and indirect) to critical infrastructure facilities (for example, water supply, electricity, healthcare, telecommunications.

At the same time, despite the academic updating, wide media coverage, and political speculation about this phenomenon, there is still the problem of conceptual and legal uncertainty of cyberterrorism as an atypical form of terrorism in general. In turn, such uncertainty generates the risks of inadequate response from the authorities in terms of the optimal (sufficient) legal regulation of relations in the field of countering current and potential cyber threats and the correct classification of computer network attacks as acts of terrorism.

MATERIALS AND METHODS

The paper is devoted to the analysis of various scientific positions considering the legal essence of cyberterrorism in modern legal thought. There is a position of certain researchers (KERSCHISCHNIG, 2012; KAPUSTIN, 2017; A. SAMUEL, 2021; PARKER, 2021) that treat this phenomenon as a destructive and aggressive action in the communication environment, which determines the terminological convergence of some related notion (cyber interference, cyberattack, cyberwar, cyber incident, cyberaggression, hacktivism). Other researchers (S. KRASAVIN, 2021; DENNING, 2021; CHERNYADIEVA, 2017), on the contrary, define this phenomenon through cyberattacks or threats of attacks against information, computer systems, computer programs and data committed for terrorist purposes. And the third group of scientists (DREMLIUGA, KOROBEEV, FEDOROV,2017) analyse cyberterrorism in an extensive format, that cover terrorist acts committed through the use of remote information.
and communication technologies on the Internet for causing harm to the public interests, and actions that are committed in support of terrorism through the malversation of the Internet.

The methodological grounds of this study are conventional scientific and special legal research methods: the analysis (which allowed highlight and study individual aspects of the phenomenon under consideration), the method of transition from abstraction to concretization (in terms of formulating a more precise definition of cyberterrorism), a method of deduction, which involves leading thought from general provisions to particular conclusions, comparative-legal and formal-legal methods are used also.

**OPTIONS FOR A WORKING DEFINITION OF CYBERTERRORISM**

Despite the wide coverage of the problems of the dissemination of cyberterrorism, combined with the low efficiency of national law enforcement systems in countering it, a single concept of this phenomenon has not yet been developed. The complexity of the phenomenon under consideration in terms of definitive identification is evidenced by the wide range of concepts of cyberterrorism presented in the academic sphere and expressing the different essence of this phenomenon. Without claiming to a substantive analysis and detailed coverage of various author’s proposals regarding this phenomenon, it seems possible for the purposes of this study to propose three approaches to defining cyberterrorism.

Firstly, cyberterrorism is often perceived from the standpoint of general ideas or particular ideas about various destructive and aggressive manifestations in the information and communication environment prevailing in the academic sphere, which predetermines the terminological convergence of such concepts as cyber interference, cyber-attack, cyberwar, cyber incident, cyber aggression, hacktivism (KERSCHISCHNIG, 2012; BLANCK, 2013; KAPUSTIN, 2017; https://cyberleninka.ru; PARKER, 2010). This approach is difficult to recognize as acceptable since it reflects an extremely broad understanding of the phenomenon, which reduces its essence and does not allow differentiation from adjacent phenomena of social reality, inspired in the information and communication space. In addition, such an approach leads (or may lead) to a blurring of the boundaries between terrorism, the crime of aggression, and computer network attacks committed with hooligan motives, which in turn can create problems of the correct qualification of such attacks without taking into account their objective social danger. In this aspect, it becomes clear why various world media outlets and representatives of state bodies of different states, without understanding the situation and without having solid evidence but guided by speculative political or ideological motives, tend to accuse one or another country of aggression, terrorism, interference in the internal affairs of another state through the use of cyberweapons.

Second, cyberterrorism is defined through unlawful attacks or threats of attacks against information, computer systems, computer programs, and data, committed for political, ideological, religious, or other reasons in order to force the authorities to assist in achieving political or social goals (http://www.crime-research.org; http://www.iwar.org.uk; CHERNYADYEVA, 2017). Cyberterrorism is a collection of illegal actions in cyberspace that contribute to the creation of fear and tension in a society in order to gain an advantage in solving political, economic, or social problems. Subsequently, the proposed definition of cyberterrorism was expanded to include non-state actors who carry out cyberattacks (or threats of such attacks) against information systems to intimidate or coerce official authorities or society in order to achieve political or social goals. This form of terrorism involves the use of computers and related equipment to cause massive disruptions in the flow of information or services, in order to create an atmosphere of fear, or undermine public confidence in key public institutions and critical national infrastructure (https://www.sipri.org; HUA, BAPNA, 2012).

Third, cyberterrorism should cover both terrorist acts committed through the use of remote information and communication technologies on the Internet to harm public interests, and actions that are committed in support of terrorism through the abuse of the Internet (DREMLIUGA et al., 2017). The latter include:

- propaganda of terrorist practices and ideology;
• persuading, recruiting, or otherwise involving a person in committing crimes of a terrorist nature;
• training of persons for terrorist purposes;
• financing of terrorism;
• justification of terrorism, as well as public calls for terrorist activity.

In addition, Internet resources can also be used to provide appropriate communications between terrorist groups and individual terrorists. The scientific literature notes that anonymous email accounts and encryption can be used to disguise terrorist communication, websites can be used to distribute propaganda or recruit members, and the Internet itself can act as a way to gather necessary information (Clough).

In general, it can be noted that the expanded approach in defining cyberterrorism is consistent with the international practice of countering terrorism in the information space. In this aspect, attention is drawn to the official approach of the UN Office on Drugs and Crime, according to which cyberterrorism covers various crimes of a terrorist nature (in particular, propaganda (the use of the Internet for recruitment, incitement and radicalization), financing, training, planning, dissemination threats, the implementation of the terrorist act itself) that are committed in the information space and (or) with the help of information and communication technologies (THE USE OF THE INTERNET FOR TERRORIST PURPOSES, 2012).

THE STATE OF INTERNATIONAL LEGAL COUNTERACTION TO CYBERTERRORISM AT THE PRESENT STAGE OF DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Before moving on to a legal analysis of cyberterrorism as an atypical form of traditional terrorism, it is necessary to reveal the concept of cybercrime as a broader (generic) concept. In the academic environment, there is no certainty on this issue, since autochthonous concepts are often used, which reveal the etymological meaning of the phenomenon under consideration, with the assumption of some conventionality in relation to the sphere used. Cybercrime is often defined through terms such as "computer crimes", "computer-related crimes", "computer assisted crimes", "information crimes". In the context of the development of information and communication technologies, one can find the identification of cybercrimes with high technologies, digital, electronic, virtual, technological and high-tech illegal acts (https://www.state.nj.us).

Such an expanded understanding of de facto cybercrime can lead to a distortion of the meaning of the phenomenon itself and, as a consequence, create difficulties in the practical application or in the prospective use of this term in the regulatory system. Indeed, if we follow the literal sense of the proposed concepts, then we can admit that computer crimes are understood exclusively as crimes that are committed through the use of personal computers, regardless of their network connection. Virtual crimes, as well as cybercrimes, can be considered as illegal acts that are committed exclusively on the Internet. High-tech crime can also extend beyond networked information technology to include other “high-tech” developments such as nanotechnology and bioengineering.

Today, there is no single international convention governing relations in the field of combating cybercrime. However, the political and legal counteraction to specific acts committed in the information space and qualified as cybercrimes is reflected in five regional conventions in the field of combating computer crimes (Council of Europe Convention on Cybercrime (ETS N 185) of 23 November 2001 (hereinafter referred to as the Council of Europe Convention) (https://www.state.nj.us), African Union Convention on Cyber security and Personal Data Protection dated June 27, 2014 (hereinafter referred to as the African Union Convention) (https://www.sbs.ox.ac.uk), Agreement on cooperation in Combating offences related to computer information dated June 1, 2001 (hereinafter referred to as the CIS Agreement) (https://base.garant.ru), The League of Arab States Convention on Combating Technology offences of 2010 (hereinafter referred to as the League of Arab States Convention) (https://www.asianlaws.org) and Agreement between the governments of state members of the Shanghai Cooperation Organization (SCO) on cooperation in the field of ensuring the
international information security of June 16, 2009 (hereinafter referred to as the SCO Agreement) (Agreement between the Governments of the Shanghai Cooperation Organization member states on cooperation in the field of international information security, 2012).

A comparative legal analysis of the above regional conventions allows us to come to the conclusion about different approaches to the legal regulation of acts as cybercrimes. On the one hand, there are general aspects of the political and legal definition of acts as computer crimes. Here, in particular, it is necessary to note a unified approach (but with the differentiation of the constitutive features of specific offenses) in identifying three groups of cybercrimes: acts against confidentiality, integrity and availability of computer data and systems; actions performed through the use of computers for personal or financial gain, as well as causing harm; acts related to computer content.

On the other hand, there are different approaches to defining crimes related to computer content (affiliated with other crimes). For example, in Art. 3 of the African Union Convention, such crimes include incitement to hatred through the use of computer technology and the production, distribution, or possession of child pornography. The Council of Europe Convention refers to such only offenses related to child pornography (Article 9). On the contrary, the agreement on cooperation of the member states of the Commonwealth of Independent States in the fight against crimes in the field of computer information does not contain such a group of crimes.

At the same time, attention is drawn to the regional experience in countering computer crimes related to terrorist activities. So, Art. 15 of the Arab League Convention discloses the legal content of terrorism-related crimes committed through information technology. Such crimes include dissemination and propaganda of ideas and principles of terrorist groups; financing and preparation of terrorist operations, as well as providing communication between terrorist organizations; the proliferation of methods of making explosives for use in terrorist operations; the spread of religious fanaticism, discord, and religious enmity. A mandatory contextual feature is a condition for the commission of these acts, which is expressed in the use of information technologies. In part 1 of Art. 2 of this document a legal definition of information technology, which means any material or virtual means, as well as a group of interrelated means that are used to store, sort, organize, retrieve, process, transform and exchange information in accordance with the commands and instructions in force in this respect is given.

The African Union Convention also contains a special rule regulating the adaptive connection between computer crimes and certain terrorist crimes. An illustrative example in this regard is the rule of clause ‘b’ of Part 1 of Art. 30 of this document, where it is determined that the participating States must take the necessary regulatory and legal measures that enshrine as an aggravating circumstance the use of information and communication technologies to commit theft, fraud, concealment of stolen property, breach of trust, extortion, money laundering and terrorism.

Of particular interest is the 2009 Agreement between the governments of state members of the Shanghai Cooperation Organization (SCO) on cooperation in the field of ensuring the international information security. Unlike the above conventions, this document provides a working definition of information terrorism, which means the use of information resources and (or) impact on them in the information space for terrorist purposes. In accordance with the second paragraph of Appendix No. 2 “List of the main types of threats in the field of international information security, their sources and signs” of the agreement under consideration, the signs of the considered threat are the use of information networks by terrorist organizations to carry out terrorist activities and attract new supporters; destructive impact on information resources, leading to disruption of public order; control or blocking of media transmission channels; using the Internet or other information networks to promote terrorism, create an atmosphere of fear and panic in society, as well as other negative impacts on information resources. This agreement is fundamentally different from other regional conventions also in the sense that it differentiates information terrorism from related threats in the field of international information security. In particular, information terrorism within the meaning of this agreement should be distinguished from information warfare, information...
crime, the use of a dominant position in the information space to the detriment of the interests and security of other countries, the dissemination of information harmful to socio-political and socio-economic systems, spiritual, moral and the cultural environment of other states, as well as from the threat to the safe, stable functioning of global and national information infrastructures of a natural and (or) man-made character.

To date, there are no special conventions in the system of public international law regulating countering cyberterrorism. However, given the ambivalence of this act (which is expressed, on the one hand, in the fact that signs of terrorism are seen in the phenomenon as a whole, and on the other hand, illegal acts are committed through the use of information and communication technologies on the Internet), it becomes appropriate to consider the international legal regulation of countering this phenomenon within the framework of the conventional mechanism for combating various types of terrorism.

The Convention Mechanism for Countering Terrorism is represented by a large number of international treaties of a universal and regional nature. Currently, 40 "anti-terrorist" international treaties have been established, including 18 treaties signed within the framework of lawmaking work under the auspices of the United Nations, and 22 regional documents. Many issues regarding interstate cooperation and the development of national measures in the fight against terrorism are reflected in special UN declarations and resolutions.

In most cases, international conventions are focused on the identification, prevention, suppression, investigation, and disclosure of terrorist crimes. However, in certain cases, acts of cyberterrorism also fall under the regulatory action of some conventions. For example, cyberattacks on IT systems or databases can have a negative impact on objects in the real world, which is explained by the functional connection between the IT system and the management infrastructure itself. For this reason, attacks on aircraft or airport IT systems fall under the definition of terrorism under the 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (http://www.consultant.ru). In particular, in paragraph “B” of Art. 2 of this document stipulates that illegal acts include actions aimed at destroying an aircraft in service, or causing damage to this aircraft, which puts it out of action or may threaten its safety in flight. Although at the time of the acceptance of the presented convention, only acts of physical behavior were considered, however, within the framework of the expanded interpretation of this norm, in principle, nothing prevents from qualifying unlawful electronic interference with the on-board power supply of an aircraft as an act of terrorism, since such actions can also threaten its safety in flight. In addition, within the meaning of this convention, unlawful acts of electronic interference with air navigation equipment that generate a threat to the safety of an aircraft in flight should also be considered as crimes of a terrorist nature (clause “d” of Part 1 of Article 1).

Cyberattacks on the control system of nuclear power plants can be classified as a terrorist act in accordance with the International Convention for the Suppression of Acts of Nuclear Terrorism of 2005, which follows from paragraph “b” of Part 1 of Art. 2 of this document: “Any person commits an offense within the meaning of this Convention if he unlawfully and intentionally uses radioactive material or device in any way, or uses or damages a nuclear facility in such a way that the release occurs or there is a risk of releasing radioactive material” (http://www.consultant.ru). Based on this formulation, it is naturally possible to make an assumption about the possible use of information and communication technologies to take possession of the entire electronic control system of a nuclear facility in order to use or damage it in order to release or create a danger of releasing radioactive material. Cyberterrorism as a form of terrorism in general also falls under the regulatory action of the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (http://www.consultant.ru). Here, attention is drawn to the norm of clause "e" of Part 1 of Art. 3 of this document, which determines that actions related to the destruction of maritime navigation equipment, as well as causing serious damage to it or causing serious interference with its operation, should be considered a criminal act, if any such act could threaten the safe navigation of the vessel. The convention does not say about the nature of such an action; therefore, it is possible to assume that not only physical actions are performed, but also remote acts of electronic interference in navigation control systems.
Meanwhile, in the system of international legal counteraction to terrorism, there are situations when cyberattacks are not directly covered by the relevant conventions, although the development of modern information and communication technologies that create new threats to the security of relevant facilities are a precursor for the prospective expansion of these conventions or the acceptance of new ones. For example, in the 1970 Convention for the Suppression of Unlawful Seizure of Aircraft (“The Hague Convention”), unlawful seizure and control of an aircraft is understood as actions involving violence, the threat of violence, or another form of intimidation. A similar approach was outlined in the 2005 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf. In paragraph “a” part 1 of Art. 2 of this Protocol stipulates that it is an offense to seize or control a fixed platform by force or threat of force or by any other form of intimidation. Meanwhile, a situation cannot be ruled out when the establishment of control in relation to an aircraft or a stationary platform can occur through electronic intervention in the control system, however, due to the direct interpretation of these provisions, the extended application of the presented convention in such situations is not permissible.

Separately, it should be said about those anti-terrorist conventions that exclude the possibility of the legal qualification of cyber-attacks due to the specificity of the subject of legal regulation. These conventions include: the 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection, which provides for chemical marking to facilitate the detection of plastic explosives, for example, to combat acts of sabotage against aircraft; 1999 Convention for the Suppression of the Financing of Terrorism, which regulates the procedure for countering the financing of terrorists and establishes obligations for states to hold criminal, civil or administrative responsibility for such acts, as well as stipulating obligations to identify, freeze and seize funds intended for terrorist activities; 1997 Convention for the Suppression of Terrorist Bombings, which provides for a regime of universal jurisdiction over the unlawful and deliberate use of explosive or other lethal devices within or against various designated public places with intent to cause death or serious injury or significant destruction of such public places; The 1979 Convention Against the Taking of Hostages, establishing measures to combat the taking or retention of another person for terrorist purposes; 1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, concerning Attacks against High Government Officials and Diplomats (https://www.un.org/ru).

However, if we proceed from a broader definition of cyberterrorism, which covers not only computer network attacks on social infrastructure facilities but also actions related to the spread of propaganda of ideas of terrorism, recruitment, financing, training of potential terrorists, and incitement to commit terrorist acts, then within this scope, it is natural to make an assumption about the possibility of extended regulatory action of a number of conventions. For example, in accordance with Part 1 of Art. 2 of the 1999 Convention for the Suppression of the Financing of Terrorism, any person commits an offense within the meaning of this Convention if this person, by any means, directly or indirectly, unlawfully and intentionally provides funds or collects them with the intention that they are used, or in the knowledge that they will be used, in whole or in part, to commit crimes of a terrorist nature. This document does not indicate the use of the Internet space in order to create funds for terrorist purposes, but such a possibility cannot be ruled out, since modern terrorist organizations are increasingly moving into the shadow segment of the Internet, where they create various kinds of resources aimed at financing terrorism. A 2013 UN Office on Drugs and Crime special report notes that terrorists use a variety of methods to mobilize and raise funds and resources (https://www.unodc.org).

These methods include, inter alia, direct requests for donations, e-commerce, the use of online payment instruments, and the mediation of charitable organizations. Direct online appeals are made through the use of websites, chat groups, mass mailings, and targeted messages to convey donation requests from supporters. Websites can also be used as online stores offering books, audio, and video recordings, and other merchandise to supporters. Fund transmitting is often made using electronic bank transfers, credit cards, or other means of payment. In turn, the use of information and communication resources in the information space for the purpose of public incitement to terrorism, as well as the recruitment and training of terrorists, may be
covered by the regulatory action of the Council of Europe Convention on the Prevention of Terrorism of 2005 (Council of Europe Convention on the Prevention of Terrorism, 2005). Although the Convention does not directly indicate the possibility of committing these crimes of a terrorist nature through the use of the Internet, in principle, nothing prevents the use of information and communication resources for the purpose of recruiting, persuading or training potential terrorists.

CONCLUSION

Based on the analysis of doctrinal ideas regarding the conceptual and legal essence of cyberterrorism and the study of the international convention mechanism for countering terrorism, as well as regional documents in the field of information security, the following conclusions can be done.

First, in the domestic and foreign doctrine, there is no generally accepted definition of cyberterrorism as a type of information threat manifested on the Internet. Analysis and generalization of scientific positions regarding the development of an optimal definition of cyberterrorism highlight only the general outlines of the phenomenon under consideration, according to which cyberterrorism is defined as the illegal use of information and communication technologies in relation to computer information, computer systems and networks in critical segments of the state and in the private sector, which create the danger of death of people, causing significant property damage or the onset of other socially dangerous consequences, with the aim of aggravating fear and tension, as well as influencing the authorities for political or other inherent in the ideology of terrorism, motives. It should be noted that in the legal field, attempts are being made to expand the understanding of cyberterrorism, encompassing both cyber-attacks against computer information, computer systems and networks, and other types of illegal activities to support terrorism through the abuse of the Internet (in particular, the propaganda of ideas of terrorism, incitement, recruitment, financing, training, planning, threat propagation) (YAKOVYUK, SHESTOPAL, 2017; SHESTOPAL et al., 2017; BYTIAK et al., 2018; YAKOVYK et al., 2018).

Second, the international regional conventions on cybercrime (2001 Council of Europe Convention; 2014 African Union Convention on Cyber security and Personal Data Protection; 2001 Agreement on cooperation in Combating offences related to computer information, 2010 The League of Arab States Convention on Combating Technology offences), reflecting the criminalization of acts, committed in the field of computer information, in some cases, consolidate the contextual connection of crimes in the field of information technology with certain manifestations of terrorism. Meanwhile, it seems that the Agreement between the Governments of the Shanghai Cooperation Organization member states on cooperation in the field of ensuring international information security from 2009 is fundamentally different from other regional conventions, since it introduces the concept of “information terrorism” and distinguishes this type of terrorism from related threats in the field of international information security.

Thirdly, in the system of modern international criminal law, there are no legal acts governing relations regarding countering cyberterrorism as a conventional crime. The existing convention mechanism for countering terrorism only in some cases allows one to consider cyberattacks in the framework of criminal law norms on traditional crimes of a terrorist nature since computer network attacks not always can determine the onset of consequences comparable to those of a traditional terrorist act. At the same time, crimes of a terrorist nature committed through the use of the Internet (propaganda of ideas of terrorism, recruitment, financing, training of potential terrorists, and incitement to commit terrorist acts) may be covered by special conventions constituting the anti-terrorist convention mechanism.

REFERENCES

AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION (Malabo, June 27, 2014). [Electronic resource]. Available at: https://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/African%20Union%20Convention%20on%20CyberSecurit y%20%26%20Personal%20Data%20Protection_1.pdf. Access: May 23, 2021.
AGREEMENT BETWEEN THE GOVERNMENTS OF THE SHANGHAI COOPERATION ORGANIZATION MEMBER states on cooperation in the field of international information security (Yekaterinburg, June 16, 2009) Bulletin of international treaties, 2012, n. 1, p. 13 - 21.

AGREEMENT ON COOPERATION IN COMBATING OFFENCES RELATED TO COMPUTER INFORMATION, 2001 [Electronic resource]. Available at: https://base.garan.ru/12123778/. Access: May 23, 2021.

ASHRAF, D.A.; FILIPPIDOU, D.A. Terrorism and Technology [Electronic resource] Centre of Excellence Defence against Terrorism. Available at: https://www.researchgate.net/publication/330039460_Terrorism_and_Technology. Access: May 23, 2021.

BLANCK, L. R. International Law and Cyber Threats from non-states Actors. Int’L L. Stud, 2013, 89 (406), p. 406-409.

BOSCH, O. Defending against cyberterrorism: preserving the legitimate economy [Electronic resource]. Available at: https://www.sipri.org/sites/default/files/files/books/SIPRI04BaiFro/SIPRI04BaiFro16.pdf. Access: May 23, 2021.

BYTIK, Y. P.; YAKOVIYK, I. V.; GETMAN, E. A.; TRAGNIUK, O. Y.; SHESTOPAL, S. S. Cooperation of former Soviet Union countries and Ukraine with the European Union. ORBIS, 2018, 14 (41), p. 46-54.

CHERNYADYEVA, N.A. International terror: origin, evolution, current issues of legal counteraction: Monograph. Moscow: Prospect, 2017, 160p.

COMPUTER CRIME. A Joint Report, 2000. [Electronic resource]. Available at: https://www.state.nj.us/sci/pdf/computer.pdf. Access: May 23, 2021.

CONVENTION FOR THE SUPPRESSION OF UNLAWFUL ACTS AGAINST THE SAFETY OF CIVIL AVIATION 1971 [Electronic resource]. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=15384#005911886845499725. Access: May 23, 2021.

CONVENTION FOR THE SUPPRESSION OF UNLAWFUL ACTS AGAINST THE SAFETY OF MARITIME 1988 NAVIGATION [Electronic resource]. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=15694#022063366524796812. Access: May 23, 2021.

CONVENTIONS AND AGREEMENTS IN THE FIELD OF COUNTERING TERRORISM [Electronic resource]. Available at: https://www.un.org/ru/documents/decl_conv/conv_terrorism.shtml. Access: May 23, 2021.

COUNCIL OF EUROPE CONVENTION “ON CRIME IN THE FIELD OF COMPUTER INFORMATION” ETS N 185 (Budapest, November 23, 2001) [Electronic resource]. Available at: https://base.garan.ru/4089723/. Access: May 23, 2021.

COUNCIL OF EUROPE CONVENTION ON THE PREVENTION OF TERRORISM (Warsaw, May 16, 2005), Collected Legislation of the Russian Federation. May 18, 2009, n. 20. Art. 2393.

DENNING, D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy [Electronic resource]. Available at: http://www.iwar.org.uk/cyberterror/resources/denning.htm. Access: May 23, 2021.

DREMLIUGA, R.; KOROBEV, A.I.; FEDOROV, A.V. Cyberterrorism in Chine: criminal law and criminological aspects. Russian Journal of Criminology, 2017, 11 (3), p. 607-614.

HUA, J.; BAPNA, S. How Can We Deter Cyberterrorism? Information Security Journal: A Global Perspective, 2012, 21 (2), p. 102-114.
INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF ACTS OF NUCLEAR TERRORISM [Electronic resource], 2005. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=4231#023195676547213195. Access: May 23, 2021.

KAPUSTIN, A. YA. On the issue of the international legal concept of threats to international information security. Journal of foreign legislation and comparative jurisprudence, 2017, 6, p. 44-51.

KERSCHISCHNIG, G. Cyberthreats and International Law. The Hague, 2012.

KRASAVIN, S. What is Cyber-terrorism? [Electronic resource]. Available at: http://www.crime-research.org/library/Cyber-terrorism.htm. Access: May 23, 2021.

PARKER, S. Cyberterrorism: An Examination of the Preparedness of North Carolina Local Law Enforcement. Security Journal, 2010, 23, p. 159-173.

SAMUEL, A. The phenomenon of hacktivism [Electronic resource]. Available at: https://cyberleninka.ru/article/n/fenomen-haktivizma/viewer. Access: May 23, 2021.

SHESTOPAL, S.; OLEYNIKOV, S.; YAKOVYUK, I. Models of the relationship between church, state and political society: Neo-Thomists' arguments. Man in India, 2017, 97, p. 499-508.

THE LEAGUE OF ARAB STATES CONVENTION ON COMBATING TECHNOLOGY OFFENCES [Electronic resource]. Available at: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf. Access: May 23, 2021.

THE USE OF THE INTERNET FOR TERRORIST PURPOSES (New York: United Nations, 2012). Pp. 3-12. [Electronic resource]. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf. Access: May 23, 2021.

USING THE INTERNET FOR TERRORIST PURPOSES: Report of the UN Office on Drugs and Crime of 2013 [Electronic resource]. Available at: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf. Access: May 23, 2021.

YAKOVIYK, I. V.; SHESTOPA, S. S.; BARANOVIK, P. V.; BLOCHINA, N. A. State sovereignty and sovereign rights: EU and national sovereignty. Opción: Revista de Ciencias Humanas y Sociales, 2018, 87p.

YAKOVIYK, I.; SHESTOPAL, S. The sovereign rights and sovereignty of the state. Azimuth of scientific research: pedagogy and psychology, 2017, 6, 4 (21), p. 381-387.
International cyberterrorism counteraction within the context of intensive development of information and communication technologies

Contrarreação internacional do ciberterrorismo reduz o contexto de desenvolvimento intensivo de tecnologias de informação e comunicação

Lucha contra el ciberterrorismo internacional en el contexto del desarrollo intensivo de las tecnologías de la información y la comunicación

Resumo
O artigo enfoca o fenômeno destrutivo do ciberterrorismo como uma manifestação (forma) atípica do terrorismo tradicional, realizado à luz do intenso desenvolvimento e ampla disseminação das tecnologias de informação e comunicação (TIC) no mundo moderno. Com base na análise de abordagens conceituais na compreensão do fenômeno em consideração, a conclusão é fundamentada que o ciberterrorismo é uma noção conceitualmente relevante (termo), que é percebida como um método de cometer um ato terrorista (entendimento truncado), ou como qualquer terrorista crimes cometidos com o uso de tecnologias de informação e comunicação (amplio entendimento). Com base em uma análise jurídica comparativa, os autores examinam as características da contra-ação regulatória e legal ao ciberterrorismo no sistema de direito penal internacional. O estudo do mecanismo da convenção internacional de combate ao terrorismo tradicional permite testar a hipótese sobre a aplicabilidade potencial de certos atos jurídicos internacionais em relação a atos socialmente perigosos cometidos por meio do uso de tecnologias de informação e comunicação para fins terroristas.

Keywords: Ciberterrorismo. Cybercrime. Segurança da informação. Ameaças da informação. Terrorismo da informação.

Abstract
The article focuses on the destructive phenomenon of cyberterrorism as an atypical manifestation (form) of traditional terrorism, carried out in the light of the intense development and wide dissemination of information and communication technologies (ICT) in the modern world. Based on the analysis of conceptual approaches in the understanding of the phenomenon under consideration, the conclusion is based on that cyberterrorism is a relevant conceptual notion (term), which is perceived as a method of committing a terrorist act (truncated understanding), or as any terrorist crime committed with the use of information and communication technologies (broad). Based on a comparative legal analysis, the authors examine as characteristics of regulatory and legal counteraction to cyberterrorism in the international criminal law system. The study of the mechanism of the international convention to combat traditional terrorism allows us to test the hypothesis on the potential applicability of certain international legal acts in relation to socially dangerous acts committed through the use of information and communication technologies for terrorist purposes.

Keywords: Cyberterrorism. Cybercrime. Information security. Information threats. Information terrorism.

Resumen
El artículo se centra en el fenómeno destructivo del ciberterrorismo como manifestación atípica (forma) del terrorismo tradicional, llevado a cabo a la luz del intenso desarrollo y la amplia difusión de las tecnologías de la información y la comunicación (TIC) en el mundo moderno. Sobre la base del análisis de los enfoques conceptuales para comprender el fenómeno que se examina, la conclusión se basa en que el ciberterrorismo es una noción (término) conceptualmente pertinente, que se percibe como un método para cometer un acto terrorista (comprensión truncada), o como cualquier delito de terrorismo cometido con el uso de las tecnologías de la información y las comunicaciones (comprensión amplia). Sobre la base de un análisis jurídico comparativo, los autores examinan las características de la lucha reglamentaria y jurídica contra el ciberterrorismo en el sistema de derecho penal internacional. El estudio del mecanismo de la convención internacional para combatir el terrorismo tradicional nos permite poner a prueba la hipótesis sobre la posible aplicabilidad de ciertos actos jurídicos internacionales en relación con actos socialmente peligrosos cometidos mediante el uso de las tecnologías de la información y las comunicaciones con fines terroristas.

Palabras clave: Ciberterrorismo. Ciberdelito. Seguridad de la información. Amenazas de la información. Terrorismo de la información.