Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/10911
DOI URL: http://dx.doi.org/10.21474/IJAR01/10911

RESEARCH ARTICLE

FEATURES OF INTERNATIONAL LEGAL COOPERATION IN COMBATING CYBER CRIME

Timur N. Butunbaev
Independent Co-Researcher for the Military Technical Institute of National Guard, Uzbekistan.

Manuscript Info

Manuscript History
Received: 05 March 2020
Final Accepted: 07 April 2020
Published: May 2020

Key words:-
International Cybersecurity, Cybercrime, Information Processing, Information Space

Abstract

Cybersecurity plays an important role in the world of information technology. Securing data is one of the biggest challenges that the governments are facing today. In this case, the first thing that has to be taken into consideration is not only the implementation of solid legal measures to fight cybercrime, but also introducing specific tools that can essentially prevent those cybercrimes on rapidly growing information space. However, the effectiveness of these measures seem questionable given the global nature of the problem, unless a solid foundation for international legal cooperation is established. Thus this article looks at the existing challenges faced by governments that are adopting international legislations and conventions against cybercrime and also discuss the potential prospects of a single global framework for international cooperation in this area.

Copy Right, IJAR, 2020,. All rights reserved.

Introduction:-

The world community is paying increasing attention to combating cybercrime, improving the resilience of cyber systems and other aspects of ensuring information security. The measures taken by various countries give an understanding of the global nature of the problem of cybercrime. Thus now cyber-attacks are paralyzing the work of not only private structures, but also of state bodies, since there is no state in the world that is fully protected from such attacks.

According to the prediction of leading cybersecurity researcher Cybersecurity Ventures “cybercrime damages will cost the world $6 trillion annually by 2021 – exponentially more than the damage inflicted from natural disasters in a year, and more profitable than the global trade of all major illegal drugs combined” (Morgan, 2019).

Indeed, in the modern world, all spheres of life are directly dependent on the work of computing and information networks. At the same time, “the widespread use of computer technology for information processing with software that makes it relatively easy to modify, copy, and destroy information” (Sachkov and Smirnova, 2015) increases the vulnerability of the information space. Users of information systems “have readily adopted Internet technology and innocently trust it while using it with the ignorance of the limitations and threats to the system security” (Sindhu et al., 2012).

For instance, the dissemination of fake information via the Internet regarding the coronavirus infection of Covid-19 in the world expert, media and political discourse became a key factor in the panic of the population, which caused a stir of demand for a number of goods.

Corresponding Author:-Timur N. Butunbaev
Address**:-**Independent Co-Researcher for the Military Technical Institute of National Guard, Uzbekistan.

At the moment, information is recognized as one of the most important values, respectively, its protection is no less important activity than its receipt and transmission. Therefore, in a "digitalized society of the beginning of the 21st century the scope of risk occurrence is changing" (Karpova, 2014).

As Stein Schjolberg, an international expert on harmonization of legislation in the field of cybercrime, noted, "Cyberspace, as the fifth common space – after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations" (2010).

The existing models of international cooperation and international law enforcement against cybercrime:-
Cybercrime is generally defined as crime in "cyberspace". Cyberspace or virtual space, in turn, can be defined as a computer-modeled information space containing information about persons, objects, facts, events, phenomena and processes, presented in mathematical, symbolic or any other form and in the process of moving through local and global computer networks, or information stored in the memory of any physical or virtual device, as well as other medium specifically designed for their storage, processing and transmission (Golubev, 2002).

When developing tools and methods to combat cybercrime, one should remember the latency of this type of crime. According to experts, the latency of "computer crimes" in the USA reaches 80%, in the UK – 85%, in Germany – 75%, in Russia – more than 90% (Vardanyan and Nikitina, 2007).

The features of the functioning of information systems "require that the joint efforts of various actors, both public and private, be directed to address cybersecurity issues" (Huey et al., 2013), yet only the state is able to effectively implement full-scale counteraction to cybercrimes, create the conditions for building the most reliable information protection systems for those who are most exposed to risks in this area.

There are examples in the world of quite effective systems to counter the commitment of cybercrime. Currently, the leading countries of the world are actively expanding and creating units in the armed forces and special services that should ensure the development of offensive capabilities in cyberspace (see the Table below) (Yakimova and Narutto, 2016).

Features of ensuring cybersecurity in a number of countries:

Country	Participation in the Convention on Cyber Security	Development of the UN Convention on International Information Security	Primary organizations in the field of cybersecurity
Great Britain	+	–	Electronic Communications Security Group at the Ministry of Foreign Affairs Legal Communications Center; The department of Virtual Threat Protection under Ministry of Defense
Germany	+	–	Special group under the Ministry of Internal Affairs of Germany
India	+	–	Foreign Intelligence Research and Analysis Wing and Internal Intelligence Bureau
China	–	+	Implementation of a program of protection against unauthorized connection to a computer
Russia	–	+	Office "K" of the Ministry of Internal Affairs and departments "K" of the regional departments of the Ministry of Internal Affairs; National contact point at the BSTE Ministry of Internal Affairs of Russia
USA	+	–	Center for National Cybersecurity; U.S. Armed Forces Cyber Command

For example, in the United States, along with the already functioning National Cyber Security Center, the Armed Forces has formed the Unified US Cyber Command, which should globally coordinate the efforts of all Pentagon structures in the course of hostilities, to provide appropriate support to civilian federal institutions, as well as interacting with similar departments of other countries (Berd, 2009). However, these organizations are partially-

controlled departments, since "the supreme controlling structure is the National Security Council with special committees whose responsibility is to implement the information strategy" (Zavyalov, 2014), including in the fight against cybercrime.

In the United Kingdom, cyber weapons programs are being implemented that will provide the authorities with the ability to withstand growing threats from cyberspace (Khimchenko, 2014).

Australia has set up an E-mail Security Coordination Group (ESCG), "the main task of which is to create a secure and reliable electronic operational space for both the public and private sectors"(Zgadzai and Kazantsev, 2013).

Activities to counter the commission of cybercrime are carried out not only by individual states, but also by their blocs, in particular by NATO. Thus the importance of this problem is reflected in all the governing documents of the bloc adopted in recent years. For the first time, the strategic concept of NATO includes a provision on cyberspace as a new area of the Alliance's military activity(Gradov, 2014).

The analysis shows that in the fight against cross-border crimes, which for the most part include cybercrimes, a special role is assigned to states, and only with well-coordinated work of law enforcement agencies of different countries can substantially reduce the number of committed crimes in this area.

International cooperation is arranged in several areas and primarily involves the creation of normative acts and the development of general recommendations, as well as the introduction of effective models of organizational interaction between states.

It should also be taken into account that the traditional mechanisms of international cooperation, including requests, mutual assistance and other similar tools used in the 21st century and earlier, are inappropriate in an era when crimes can be committed from anywhere in the world at the speed of light(Smith et al., 2004).

Legal regulation of the issues of combating cybercrime is the basis of the entire system of combating cybercrime. The complexity of the development of international acts as a whole in the situation under consideration is further complicated by the fact that "existing laws are difficult to apply when it comes to global-scope attacks that cannot be localized, the evidence of which is scattered and virtual" (Zhilina, 2003).

The international community at various levels has developed a series of acts that are relevant to the fight against cybercrime, with regional acts playing a special role, since it is currently difficult to create a global document. At the same time, it is important to note the attempts of governments to extend the norms of global international agreements to the fight against cybercrime or to conclude new agreements. For example, since organized crime groups can act alongside individuals in cyberspace, it is possible to apply international agreements to them to combat organized crime, in particular the UN Convention against Transnational Organized Crime of November 15, 2000.

In addition, the concept of the UN Convention on International Information Security was developed (2011), which was presented to the international community in November 2011 at the conference on cyberspace in London and includes the preamble, 23 articles, which are united in the main part, and final provisions. The main part of the document consists of five chapters, the contents of which are in a single compositional integrity. More importantly, Article 4 of the Convention fixes the main threats to international peace and security in the information space, of which 11 basic and 4 additional ones were broadly highlighted. Among the basic ones are listed, for example, the use of information technologies and means for carrying out hostile acts and acts of aggression; targeted destructive impact in the information space on the critical structures of another state; cross-border dissemination of information that contradicts the principles and norms of international law, as well as national laws of states. Again, the document does not indicate such real threats to international security as the commission of cybercrime, the spread of narcotic and psychotropic drugs, their analogues, as well as pornography, including child pornography.

Moreover, the concept of the Convention contains Article 5, dedicated to the basic principles of ensuring international information security. The analysis of the presented principles allows us to conclude that they can be divided into four groups: the principles of state participation in the system of international information security as a member of the international community; principles allowing the state to maintain its sovereignty in the process of

international cooperation in the fight against cybercrime; principles of ensuring free information exchange between countries. The fourth group of principles establishes the nature of the interaction of the state and private entities in the relations under consideration. At the same time, we again have to admit that the concept of the Convention does not point out the principles of international cooperation in the fight against cybercrime, except for those directed against acts of a terrorist nature.

It is good to note the inclusion of chapter 5 on "International cooperation in the field of international information security", however, the measures of international cooperation in this area seem to be insufficient for the effective functioning of the system of international economic security, since they imply only "the exchange of national concepts for ensuring security in the information space, the rapid exchange of information about crisis events and threats in the information space and measures taken in relation to their settlement and neutralization"," advice on activities in the information space, which may cause concern of the participant states, and cooperation with regard to conflict resolution of a military nature". However, these forms do not take into account the need to meet the requirement for operational cooperation between law enforcement agencies on a wide range of issues.

Thus, the provisions of the concept of the UN Convention on ensuring international information security are quite compromise in nature and are focused primarily on the prevention of information wars and terrorism.

It should be noted that most of the specialized acts to combat cybercrime are acts of the European Union, which has one of the most developed information security systems in the world. So, in October 1999, during the Tampere meeting of the European Council, it was decided to include high-tech crime in the number of crimes for which it is necessary to develop a common European approach in terms of criminalization and sanctions (Smirnov, 2012).

In 2001, the European Commission submitted a special message, "Creating a Safer Information Society byImproving the Security of Information Infrastructures andCombating Computer-related Crime" (2001), which contained legal and organizational proposals to combat cybercrime in the European Union.

The Convention on Cybercrime (2001), which governs the global response to cybercrime, adopted by the Council of Europe in 2001, is of fundamental importance to both the European Union and the entire world community.

In the preamble to the Convention, the participating states outlined the goal of its adoption – to develop, as a matter of priority, a common policy in the field of criminal law aimed at protecting society from cybercrime, including through the adoption of relevant legislative acts and the strengthening of international cooperation; restraining actions against the confidentiality, integrity and accessibility of computer systems and networks and computer information, as well as against the abuse of such systems, networks and information, by ensuring the criminal punishment of such acts and by providing sufficient powers to effectively combat these criminal offenses, by promoting the identification and investigation of such criminal offenses and the prosecution of their commission both at the domestic and international levels, and by providing arrangements for fast and reliable international co-operation.

The Convention on Cybercrime involves the implementation of actions at the level of member states and at the international level. At the national level, the development of primarily substantive criminal law is conceived: the development of provisions on crimes against confidentiality, integrity and accessibility of computer systems, networks and information, crimes related to the use of computer tools, data content, copyright infringement and related rights; determination of additional types of responsibility and sanctions (inclusion in the structure of crimes of such types as attempted commission of a crime, complicity in it or incitement to commit it in the field under consideration); establishing criminal liabilities of legal entities, which, however, contradicts the concepts of criminal liability in a number of countries, for example, in the Republic of Uzbekistan.

Thus, in the Convention on Cybercrime, cybercrimes are classified as follows:

1. Crimes against the confidentiality, integrity and access of computer data and systems: illegal access; illegal interception; data interference; system interference; misuse of devices;
2. Computer-related offences: computer-related forgery; computer related fraud;
3. Content-related offences – offences related to child pornography;
4. Offences related to infringements of copyright and related rights.

The Additional Protocol to the Convention on Cybercrime (2003) includes the following types of crimes in this list:

1. Dissemination of racist and xenophobic material through computer systems;
2. Racist and xenophobic motivated threat;
3. Racist and xenophobic motivated insult;
4. Denial, extreme minimization, approval or justification of genocide or crimes against humanity.

The Convention also implies the development of criminal procedural legislation, for example, the need for legislative consolidation of the operational security of the accumulated computer data, the search and seizure of stored computer data.

Particular attention in the Convention is paid to international cooperation, this issue is devoted to Ch. 3. The general principles of international cooperation are: the general principles of mutual assistance; the possibility of cross-border access to stored computer data with the appropriate consent or to publicly available data, mutual assistance in connection with the assessment of stored electronic data, mutual legal assistance in collecting real-time data on flows; creation of 24/7 network.

Despite the presence of other international acts in this area, "the Convention is the only recognized international treaty ... contains substantive and procedural law in order to counter cybercrime and protect freedom, security and human rights on the Internet" (Khimchenko, 2014).

The provisions of the Convention provide the basis for interaction between states, however, as the Bulgarian researcher R. Georgieva notes, "The Convention does not guarantee the security of virtual space. Of great importance will be its coordination with the domestic legislation of each country"(Georgiyeva, 2001).

Within the European Union, a number of programs are being implemented that contribute to the fight against cybercrime, and joint positions are being developed on this issue. In particular, the Stockholm program recommends the preparation of an internal security strategy for the EU in order to improve the protection of citizens and to combat organized crime and terrorism.

At the regional level, in addition to the Convention on Cybercrime, an Agreement was also adopted on cooperation of member states of the Commonwealth of Independent States in the fight against computer information crimes of June 1, 2001. The main idea of these documents is "to determine the uniformity of computer crimes that states should include in their national legislation, as well as the development of measures to combat them.

The treaties under consideration play a very important role: they established the foundations of the jurisdiction of states in criminal matters on the Internet and the rules of international cooperation, ensuring the coherence of the actions of states in the fight against computer crimes. Despite certain flaws in the treaties, in general they imply a system of interconnected international and national measures to combat computer crimes" (Talimonchik, 2013).

It is important to note that the interaction of states in the fight against cybercrime requires a generalization of the legal norms of various states in regulating the actions of the parties in the process of applyingmeasures in the fight against cybercrime. In particular, the NATO Center for Excellence in Computer Security has issued a collection of recommendations entitled "Tallinn Guidelines for the Application of International Law in Cyber War." The main tasks are the adaptation of existing legal norms in relation to armed conflicts to the specifics of hostile activities in the virtual space and an attempt to develop definitions of basic concepts in the field of computer security.

The second form of cooperation between states in the fight against cybercrime is the creation of specialized bodies.

Since the state's information security is connected with its sovereignty, the creation of a single body that would coordinate the interaction of states to combat cybercrime is difficult, but assisting bodies are being created that are guided by common standards of activity that generalize the practice of different countries on combating cybercrime.

Of great importance in the interaction of the member states of the European Union is the activity of Europol and Eurojust, who are directly involved in the fight against cybercrime in the European Union. Europol's activity uses a system of analysis work files, which are generated from data concentrated in its information system for analysis purposes, defined as processing or using data to support criminal investigations. The current analytic file system includes Cyborg (cybercrime) and Twins (child pornography) file cabinets (Volevodz, 2010).

As for Eurojust, its activities to ensure security in Europe are becoming increasingly visible: if in 2015 it investigated 2,311 cases, then in 2019the figure already reached 3,892 cases (Eurojust, 2019). Eurojust, among other things, coordinates the actions of law enforcement agencies of various states on the investigation of cybercrimes, assists in conducting investigations at the request of the relevant public authority of the member states of the European Union, and provides law enforcement agencies of these countries with information about ongoing investigations into cybercriminals.

The enforcement powers of Eurojust also extend to the initiation of criminal investigations or the submission of proposals on their initiation to the law enforcement authorities of the EU member states and the subsequent coordination of ongoing investigations.

In addition to these bodies with jurisdictional competence in this area, assisting bodies are also being created by the European Union. So, on January 18, 2013, the European Center for Combating Cybercrime was officially launched in The Hague. The goals of its creation are to collect and process data on cybercrime, conduct expert assessments of Internet threats, develop and implement advanced methods for the prevention and investigation of cybercrime, train new personnel, provide assistance to law enforcement and judicial authorities, as well as coordinate joint actions by stakeholders to increase level of security in European cyberspace (Ivanov and Tomilo, 2013).

The military interaction of states also requires resolving the issue of their cooperation in the field of organizational support for the fight against cybercrime. So, in 2008 “at the initiative of Estonia, a center of excellence for NATO was created in Tallinn, and now it is a research and educational institution of the alliance that is developing key directions for developing coalition capabilities for action in cyberspace” (Gradov, 2014).

The creation of this center was not the only area of work aimed at organizing the fight against cybercrime in the Alliance: in 2013, the deployment of a unified NATO system for responding to computer threats was completed, including two centers for responding to threats in cyberspace (in Brussels and Mons). Besides, steps are being taken to test the effectiveness of the already created system for repelling cyber-attacks, for example, the Cybercoalition and the Defense Ball learning practices are held annually.

In other words, the current trend in the international response to cybercrime is to expand the scope of interaction between states. The operational cooperation of law enforcement agencies in the fight against cybercrimes (Interpol, Europol, Eurojust), the creation and use of a single database of cybercriminals, about committed and planned cybercrimes, is becoming a reality.

Some scientists note that the work of Interpol in terms of information processing efficiency is less effective than specialized organizations of a smaller scale. Thus, Russian law enforcement agencies more often use the capabilities of the National Contact Point under the Bureau of Special Technical Events of the Ministry of Internal Affairs of Russia, which operates in a 24/7 format and is designed to provide interaction with colleagues from near and far abroad. An officer of the special forces of one of the countries at any time of the day can quickly contact the same point in another state and receive or transmit the necessary information required for conducting operational search measures. Today, national contact points operate in nearly 50 countries.

Conclusion:-

In summary, the following conclusions can be made. Given the complexity and danger of cybercrime, it is necessary to develop joint actions by legal scholars, primarily lawmakers, and, of course, information technology specialists aimed at combating crimes in global information networks. Since the introduction of normative acts of both a national and international nature is not a sufficient step towards solving the problem of combating cybercrime, in this case, special knowledge in the field of information technology and software is required.

A single global act regulating the procedure for countering cybercrimes has not been developed yet, however, the international community, in the framework of regional cooperation, is taking measures to legislatively regulate the actions of entities in cyberspace and to combat cybercrime.

References:-

1. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg, 28.1.2003. Available at: https://www.coe.int/en/web/ conventions/full-list/-/conventions/treaty/189
2. Berd, K. (2009). A war with many unknown quantities. Computerra, 2009, no.20, pp. 26-29 (In Russian).
3. 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, 26.1.2001. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52 000DC0890&from=EN
4. Convention on Cybercrime. Budapest, 23.11.2001. Available at: http://conventions.coe.int/Treaty/RUS/Treaties/ Html/185.htm
5. Convention on International Information Security (concept). Available at: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB 6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB
6. Eurojust casework 2015-2019 (Eurojust infographics). Available at: http://www.eurojust.europa.eu/doclibrary/corporate/Pages/Eurojust-Infographics.aspx
7. Georgiyeva R. Konventsiyazakiberprest"pnostta. Obshchestvo i pravo [Society and Law] Sofia, 2001, no. 11, p.16. (In Bulgarian).
8. Golubev V.A. "Kiberterrorizm" – mifilirealnost? ["Cyber-terrorism" – myth or reality?]. Available at: http://www.crime-research.ru/library/terror3.htm
9. Gradov A. The activities of the North Atlantic Treaty Organization in the sphere of cyber-security. Zarubezhnoevoennoeobozrenie [Foreign Military Review], 2014, no. 7, pp. 13-16 (In Russian).
10. Gradov A. The activities of the North Atlantic Treaty Organization in the sphere of cyber-security. Zarubezhnoevoennoeobozrenie [Foreign Military Review], 2014, no. 7, pp. 13–16. (In Russian).
11. Huey L., Nhan J., Broll R. Uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime. Criminology and Criminal Justice, 2013, vol. 13, no. 1, pp. 81-97. DOI:10.1177/1748895812448086
12. Ivanov, S. and Tomilo, O. (2013).Kiberterrorizm: ugrozanatsional'noy i mejdunarodnoybezopasnosti [Cyberterrorism: national and international security threats] Available at: https://www.arms-expo.ru/news/archive/kiberterrorizm-ugroza-nacional-noy-i-mezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/
13. Karpova D.N. Cybercrimes: a global issue and its solution. Vlast [The Power], 2014, no.8, pp. 46-50 (In Russian).
14. Khimchenko I.A. Informatsionnoeobshchestvo: pravovyeproblemy v usloviyakhglobalizatsii. Kand. Diss. [Information society: legal basis in the conditions of globalization. Cand. Diss.]. Moscow, 2014, 174 p.
15. Khimchenko I.A. Informatsionnoeobshchestvo: pravovyeproblemy v usloviyakhglobalizatsii. Kand. Diss. [Information society: legal basis in the conditions of globalization. Cand. Diss.]. Moscow, 2014. 174 p.
16. Morgan, S. (2019). 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Available at: https://cybersecurityventures.com/cybersecurity-almanac-2019/
17. Sachkov D.I., Smirnova I. G. Obespechenieinformatsionnoibezopasnosti v organakhvlasti [Ensuring Information Security in the Bodies of Power]. Irkutsk, Baikal State University of Economics and Law Publ., 2015, 122 p.
18. Schjolberg Stein. A cyberspace treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010. Available at: http://cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf
19. Sindhu K.K., KombadeRupali, GadgeReena, Meshram B.B. Forensic Investigation Processes for Cyber Crime and Cyber Space. Proceedings of International Conference on Internet Computing and Information Communications, 2012, vol. 16, pp. 193-206.
20. Smirnov A.A. EU System of Fight against Cybercrime. Bibliotekakriminalista [Criminalist's Library], 2012, no. 2 (3), pp. 262-274 (In Russian).
21. Smith R.G., Grabosky P., Grabosky G. Criminals on Trial. Cambridge University Press, 2004. 263 p.
22. Talimonchik V.P. Mezhdunarodno-pravovoeregulirovanieotnosheniy v sfereinformatsii. Avtoref. Dokt. Diss. [International legal regulation of relations in the sphere of information. Doct. Diss. Thesis]. Saint Petersburg, 2013. 52 p.

23. Vardanyan A.V., Nikitina E.V. Rassledovanieprestupleniy v sferevisokikhtekhnologiy i kompyuternoyinformatsii [Investigation of Hi-Tech and Computer Information Crimes]. Moscow, Yurlitinform Publ., 2007, 307 p.
24. Volevodz A.G. Uchrezhdeniya i organyEvropeiskogosoyuzaposudebnomu i politseiskomusotrudnichestvu [Agencies and Bodies of the EU on court and police cooperation]. Moscow, European Studies Institute at MGIMO-University Publ., 2010. 303 p.
25. Yakimova E.M., Narutto S.V. International cooperation in cybercrime counteraction. Criminology Journal of Baikal National University of Economics and Law, 2016, vol. 10, no.2, pp. 369-378. DOI: 10.17150/1996-7756.2016.10(2).369-378. (In Russian).
26. Zavyalov S. International experience in fighting the propaganda of terrorism in the Internet. Zarubezhnoevoennoeobozrenie [Foreign Military Review], 2014, no. 4, pp. 34-39 (In Russian).
27. Zgadzai O.E., Kazantsev S.Ya. Cybercrime: factors of danger and problems of struggle. Vestnik GU "Nauchniytsentrbezopasnostizhiznedeyatelnostidetey" [Bulletin of "Research Center for the Security of Children"], 2013, no. 4 (18), pp. 80-86 (In Russian).
28. ZhilinaI.Yu. Cybercrimes and counteracting them (a summary). Sotsialniye i gumanitarniyenauki. Otechestvennaya i zarubezhnayaliteratura. Seriya 2, Ekonomika [Social and Humanitarian Science. Russian and Foreign Literature. Series 2, Economics], 2003, no.1, pp. 144-148 (In Russian).