IRSTI 10.77.51

Tatarinova L.[1], Dzhanadilov O.[2], Tatarinov D.[3]

[1]PhD in Law, Associate professor of the department «Jurisprudence and international law», «Turan» University, Kazakhstan, Almaty, e-mail: dove_2003@mail.ru
[2]PhD student, in «Jurisprudence» of the Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan, Kazakhstan, Astana, e-mail: olzhas.dzhanadilov@mail.ru
[3]PhD in Law, senior lecturer of the international law department, Al-farabi Kazakh National University, Kazakhstan, Almaty, e-mail: danila_tatarinov@mail.ru

CONCEPTUAL PROBLEMS OF DEFINING MAIN TYPES OF OFFENSES IN THE SPHERE OF INFORMATIZATION

The article is devoted to the conceptual problems of determining the main types of offenses in the field of informatization in terms of the norms of international law and the national legislation of the Republic of Kazakhstan. The authors attempted to disclose the legal nature of each of the known criminal laws of unlawful acts committed through IT technologies in the field of information. The results and conclusions have a high practical importance, since they can be taken as a basis for qualifying acts as offenses in the field of informatization.

This study was conducted through active application of both general scientific and private scientific methods of cognition. The method of comparative analysis was actively used, by means of which the authors compared existing approaches to the topic under study that take place in the science of international law and criminal law of the Republic of Kazakhstan. Of particular importance in this study is the use of the statistical method, which made it possible to establish with scientific certainty which kinds of offenses are taking place in global communication networks, to pay due attention to solving organizational problems of detecting and identifying offenders in the field of global communication networks on an international scale through operational search events.

Accordingly, this study is aimed at filling the existing gaps in the field of understanding the legal nature of the main types of offenses in the field of information.

Key words: offenses, types, informatization, IT-technologies, cybercrime.

Татаринова Л.[1], Джанадилов О.[2], Татаринов Д.[3]

[1]з.ғ.к., «Туран» Университеті, құқықтану және халықаралық құқық кафедрасының доценті, Қазақстан, Алматы қ., e-mail: dove_2003@mail.ru
[2]Қазақстан Республикасы Бас прокуратурасының Құқық қорғау органдары Академиясының «Құқықтану» мамандығы бойынша PhD докторанты, Қазақстан, Астана қ., e-mail: olzhas.dzhanadilov@mail.ru
[3]з.ғ.к., халықаралық құқық кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан, Алматы қ., e-mail: danila_tatarinov@mail.ru

Ақпараттандыру саласындағы құқық бұзушылықтардың негізгі түрлеріне анықтама берудің концептуалды проблемалары

Мақала халықаралық құқық нормалары мен Қазақстан Республикасының ұлттық заңнамасы бойынша ақпарат саласындағы құқық бұзушылықтардың негізгі түрлерін анықтаудың тұжырымдамалық мәселелеріне арналған. Авторлар ақпарат саласындағы IT-технологиялар арқылы жасалынған заңсыз әрекеттердің әрқайсысы белгілі қылмыстық құқықтың заңды сипатын ашуға тырысты. Қол жеткізілген нәтижелер мен қорытындылар жоғары практикалық маңызға ие, өйткені олар біліктілік актілеріне ақпараттандыру саласындағы құқық бұзушылық ретінде негіз болуы мүмкін.

Бұл зерттеу танымның жалпы ғылыми және жеке ғылыми әдістерін белсенді қолдану арқылы жүзеге асырылады. Салыстырмалы талдау әдісі белсенді қолданыла отырып, оның көмегімен авторлар халықаралық құқық пен Қазақстан Республикасының қылмыстық құқығы ғылымында

қарастырылған тақырыпқа қолданыстағы тәсілдерді салыстырды. Зерттеу барысында жаһандық коммуникациялық желілерде құқық бұзушылықтардың түрлері болып табылатын ғылыми сенімділікті қалыптастыруға мүмкіндік беретін статистикалық әдісті қолданып, жаһандық коммуникациялық желілерде құқық бұзушыларды анықтау және анықтауды ұйымдық мәселелерді халықаралық деңгейде тез арада шешу арқылы ұйымдастырылады.

Тиісінше, бұл зерттеу ақпарат саласындағы құқық бұзушылықтардың негізгі түрлерінің заңды сипатын түсіну саласындағы қолданыстағы кемшіліктерді толтыруға бағытталған.

Түйін сөздер: құқық бұзушылықтар, түрлері, ақпараттандыру, IT-технологиялар, киберқылмыс.

Татаринова Л.[1], Джанадилов О.[2], Татаринов Д.[3]

[1]к.ю.н., Университет «Туран», доцент кафедры юриспруденции и международного права, Казахстан, г. Алматы, e-mail: dove_2003@mail.ru

[2]докторант PhD по специальности «Юриспруденция», Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, Казахстан, г. Астана, e-mail: olzhas.dzhanadilov@mail.ru

[3]к. ю.н., ст. преподаватель кафедры международного права, Казахский национальный университет им. аль-Фараби, Казахстан, г. Алматы, e-mail: danila_tatarinov@mail.ru

Концептуальные проблемы определения основных видов правонарушений в сфере информатизации

Представленная статья посвящена концептуальным проблемам определения основных видов правонарушений в сфере информатизации с точки зрения норм международного права и национального законодательства Республики Казахстан. Авторы предприняли попытку раскрыть правовую природу каждого из известных науке уголовного права противоправных деяний, совершаемых посредством IT-технологий в сфере информатизации. Результаты и сделанные выводы имеют высокую практическую значимость, поскольку могут быть взяты за основу при квалификации деяний, как правонарушения в сфере информатизации.

Данное исследование проведено посредством активного применения как общенаучных, так и частно-научных методов познания. Активно применялся метод сравнительного анализа, с помощью которого авторы сравнили существующие подходы к исследуемой теме, имеющие место в науке международного права и уголовного права Республики Казахстан. Особое значение при данном исследовании имеет применение статистического метода, что дало возможность с научной достоверностью установить, какие именно виды правонарушений имеют место в глобальных коммуникационных сетях, обратить должное внимание на решении организационных проблем обнаружения и идентификации правонарушителей в сфере глобальных коммуникационных сетей в международном масштабе посредством оперативно-розыскных мероприятий.

Соответственно, данное исследование направлено на восполнение имеющихся пробелов в сфере понимания правовой природы основных видов правонарушений в сфере информатизации.

Ключевые слова: правонарушения, виды, информатизация, IT-технологии, киберпреступления.

Introduction

The continuous development of information technologies has led to the fact that all spheres of human life are connected in one way or another with computer technologies and global communication networks. It should be noted that it was the active development of IT technologies that led to the emergence of new types of crimes in the modern world – computer crimes.

A notable feature of computer crimes is also their transnational nature. The boundaries between countries, the distance, the difference in the languages of communication are no longer of great importance. Determining factors are the level of computerization of society, the ability to access computers, relevant specialized knowledge common to programmers from different countries. Thus, it means the need for the unification of legal norms on computer crimes and the need for a constant reference to the foreign experience of combating computer crimes when creating national legal norms.

1. Problems of definition of the term «infringements in the field of informatization» in the narrow sense.

The criminal code of the Republic of Kazakhstan passed transformation, which required the adoption of a new wording which came into force on 1 January 2015. In this edition, have been implemented new developments in the evolution of the science of criminal law and criminology, some acts have been revised, taking into account international problems.

Reforms did not ignore such a sphere as computer technologies and informatization. Earlier, the responsibility for crimes in this sphere was provided for by Article 227 of the Criminal Code of the Republic of Kazakhstan (Criminal Code of RK, 1997). However, in connection with the constantly evolving computer technologies, the problem of reviewing the dispositions and, accordingly, sanctions for illegal acts committed through IT technologies, has acquired special relevance.

Like all crimes, they are subdivided into species depending on the object, on the subject of encroachment, depending on the methods of commission, etc. (Tropina, 2005: 44).

When considering the issue of the main types of IT crimes, it should be noted that these crimes are divided into computer crimes and crimes committed through global communication networks that allow access to cyberspace (Brazhnik, 2003:27).

This classification is also used by the UN, dividing this type of criminal activity into cybercrime in a «broad» and «narrow» sense. This classification also corresponds to the division of computer crimes into single-object and multi-object (Mitskevich, 2004: 19).

In this regard one can not but agree with the opinion of T.D. Tropina, who notes that: «Computer crimes in the narrow sense are crimes, the main object of encroachment of which is confidentiality, integrity, accessibility and safe functioning of computer data and systems.

Computer crimes in a broad sense are crimes that, in addition to computer systems, infringe upon other objects (as the main ones): the security of society and human (cyberterrorism), property and property rights (thefts, fraud committed by computer systems or cyberspace), copyrights (plagiarism and piracy) « (Tropina, 2005: 44).

Computer crimes in a broad sense are crimes that, in addition to computer systems, infringe on other objects (as the main ones): security of society and human (cyberterrorism), property and property rights (theft, fraud committed by computer systems or in cyberspace), copyright rights (plagiarism and piracy) « (Tropina, 2005: 44).

So, according to the current criminal legislation of the Republic of Kazakhstan, criminal offenses in the sphere of informatization are:

– Illegal access to information, to the information system or telecommunications network (art. 205 of the Criminal Code of the Republic of Kazakhstan);

– Illegal destruction or modification of information (art. 206 of the Criminal Code of the Republic of Kazakhstan);

– Violation of the operation of the information system or telecommunications networks (art. 207 of the Criminal Code of the Republic of Kazakhstan);

– Illegal acquisition of information (art. 208 of the Criminal Code of the Republic of Kazakhstan);

– Coercion to transfer information (art. 209 of the Criminal Code of the Republic of Kazakhstan);

– Creation, use or distribution of malicious computer programs and software products (art. 210 of the Criminal Code of the Republic of Kazakhstan);

– Illegal distribution of electronic information resources of limited access (art. 211 of the Criminal Code of the Republic of Kazakhstan);

– Provision of services for the placement of Internet resources pursuing unlawful purposes (art. 212 of the Criminal Code of the Republic of Kazakhstan).

The full list of cybercrimes is provided in the Council of Europe Convention on Cybercrime. As noted, the articles of the Convention currently cover virtually all existing illegal activities in cyberspace (Ugolovnyiy kodeks Respubliki Kazahstan, 2015).

Thus, this convention defines five types of computer crimes in a «narrow» sense:

1. illegal access (Article 2);

2. illegal interception (Article 3);

3. interference in data (violation of integrity) (Article 4);

4. intervention in the system (Article 5).

5. Illegal use of devices -

(a) production, sale, purchase for use, import, wholesale or other forms of use:

(i) devices, including computer programs, developed or adapted, primarily for the purpose of committing the offenses referred to art. 2 – 5;

(ii) computer passwords, access codes or other similar data by means of which access to the computer system as a whole or any part thereof may be obtained, with the intention of using them for the purpose of committing crimes as specified in art. 2 – 5;

(b) possession of one of the items mentioned above, with the intention of using it for the purpose of committing the crimes specified in art. 2 – 5 (article b) (Foltz C Bryan, 2004: 154).

In this regard, it is important that civilized society is seriously concerned with the problem of combating these types of crimes. This is devoted by the report of the Council of Europe, dedicated to the challenges of cybercrime, i.e. in the classification of cybercrime created on the basis of the above-mentioned Convention, this type of crime is designated as «CIA-offences», i.e. Confidentiality, integrity (Integrity) and the availability of computer data and systems (Marko Gerke, 2009).

Among the specific crimes included in this category are computer hacking, interception of messages, deception of Internet users (for example, through spoofing, phishing), computer espionage (including the use of Trojan horses and other technologies), computer sabotage and extortion (for example, the use of viruses and worms, DOS attacks, spamming and mailbombing) (Dhillon,2004: 557).

2. Problems of definition of the term «offenses in the field of informatization» in a broad sense.

As already noted earlier in this article, in addition to crimes in the «narrow» sense, there are crimes in the «broad» sense:

1. Computer-related offenses:

– computer forgery (Article 7), including online grooming;

– computer fraud (Article 8).

2. Crimes related to content (content of data) to which child pornography is attributed (Article 9).

According to the report of the Council of Europe, this crime also includes: «help» with advice, incitement, providing instructions and suggestions for the commission of a crime, including murder, rape, torture, sabotage and terrorism. This category also includes cyberbullying, libel, spreading false information through the Internet and gambling through the Internet. (Skoromnikov, 2010: .218).

3. Offenses related to violation of copyright and related rights. Types of such crimes are not singled out in the Convention; their establishment is referred by the document to the competence of national legislations of the states;

4. At the beginning of 2002, a protocol was adopted to the Convention, adding to the list of crimes the dissemination of information of a racist and other nature inciting to violence, hatred or discrimination of an individual or a group of individuals based on race, nationality, religion or ethnicity. The report of the Council of Europe assigns this group of crimes to crimes related to the content of data (Coleman C., 2003:95, Richardson R.,1998: 108).

However, it is worth acknowledging that in the convention we are considering, not all crimes are envisaged, it concerns crimes against private life. This gap was filled by the Report of the Council of Europe, which singled out crimes such as encroachment on private life, including illegal access to systems containing personal data, collecting, distributing and combining personal data or collecting data via cookies, web bugs and other software.

When considering all these types of computer crimes, in a narrow and broad sense, it is not difficult to see that they are all information crimes, because all of them, somehow, as some authors have noted, impose on information security, relations, are their additional object, and also have information in the quality of the crime subject or information influence as a way of committing a crime (Beardwood John P., Alleyne Andrew C., 2006: 62, Shinder, Debra L., 2003:136).

Computer crimes in a broad sense are the traditional types of crimes committed using a computer. These types of crimes, as shown above, are specifically identified in the Convention and are considered along with computer crimes in the narrow sense.

Analyzing the legislations of foreign countries, we found that it was changed in such a way that along with traditional types of crimes, many chapters of their criminal laws contain separate norms on committing crimes using computer means (Shils A., 1956: 163). This approach seems more justified than the approach applied within the framework of the current national legislation of the Republic of Kazakhstan, when an act committed using computer means is qualified for a combination of crimes, traditional and computer, and is punished more severely than the same act committed traditional ways.

3. The legal nature of offenses in the field of informatization in accordance with the national legislation of the Republic of Kazakhstan and some foreign states.

Nowadays, computer technologies have penetrated practically in all spheres of our life and have become quite commonplace, therefore the approach, when a more severe punishment is applied for committing a traditional crime using electronic means, is not adequate to modern reality (Ealy, A.,16).

In this regard, it is worth to agree with the opinion of A.F. Mickiewicz and S.S. Medvedev, who argue that criticism can also be subjected to proposals for the introduction of traditional crimes that qualify the use of computer tools (Mitskevich A.F., 2004: 19; Medvedev S.S., 2008: 67). This is due to the fact that the implementation of such reforms will contribute to an unreasonable increase in criminal responsibility, and also not be able to reflect the specifics of this type of crime.

Thus, computer crimes in the broad sense are an independent category of crimes possessing more features of computer crimes than traditional types of crimes.

However, it should not be mistaken that only the criminal legislation of Kazakhstan improperly

improves the norms of the Criminal Code aimed at combating crimes in global communication networks. The Russian criminalists also pay attention to such shortcomings of the legislative regulation of computer crimes in a broad sense. In particular, B.D. Zavidov conducted a criminal legal analysis of fraud in cellular networks, which can be considered as a special case of computer fraud.

In his conclusions, the scientist noted the need to improve the current legislation on liability for this type of fraud.

Finally, B.V. Zavidov noted the need to use foreign experience in the fight against electronic fraud, where these acts have long been provided for by criminal legislation and there are established methods of investigating such crimesIn particular, it was about Art. 326 of the Criminal Code of Holland, «Theft through deception of services,» which establishes responsibility for using the service offered to the public through telecommunications, using technological means or by using false signals to evade full exploitation. In addition, the author points out that the development of the infrastructure of market relations has a certain effect on fraud, which is becoming more and more new, as it were, «varieties» and «subspecies». Legislation does not manage to track their rapid development, let alone regulate, because some forms of fraud (for example, theft of funds using a computer) do not fit into its standard framework (Zavidov B.D., 1998: 16; Brenner Susan W., 2004: 19).

Thus, it becomes obvious the need for the latest developments in the field of information technology and timely changes at the legislative level to effectively combat computer crimes in a broad sense.

In the legislation of Kazakhstan, infringements in the field of informatization are narrowly defined by the norms contained in Chapter 7 of the Criminal Code of the Republic of Kazakhstan. This chapter is a revised version of the legislation, which absorbed the existing experience of criminal law regulation of relations in the field of information, but it should be recognized that information technologies are developing quite actively, which requires constant and timely improvement of the criminal legislation of the Republic of Kazakhstan.

In these norms, the offenses are closed on such actions as: illegal access to computer information, creation, use and distribution of malicious programs for computers, improper modification of the identification code of a cellular subscriber unit, subscriber identification devices, as well as the creation, use, distribution of programs for changing the subscriber unit identification code (Nurpeisova A.K., 2010: 64).

The family object of the crimes in question are public relations for ensuring public safety and public order; Species object – public relations that provide a normal mode of storage, processing and transmission of data in computers (computer systems); an additional object – public relations to ensure information security (Biebaeva A.A., 2007:137). Data is subject of the compositions in question. The result of illegal actions in the commission of computer crimes are loss of confidentiality, violation of integrity and loss of access to facilities (equipment) and data (N. Polevogo, 1998:127; Furnell S.M., Kamini Dashora).

Thus, the investigated compositions of the offenses contained in Chapter 7 of the Penal Code of the RK are the compositions of infringements of an informational nature, namely: the composition of computer crimes in a narrow sense, which is exactly what is called in the norms of international and European law.

It should be emphasized that considering the legal nature of offenses in the field of information, one can not but emphasize that these offenses, under the legislation of many foreign countries and the norms of international and European law, are classified as «computer crimes» and / or «cybercrime».

In this regard, we can state that such adjustments to existing criminal legislation are necessary, such as the legislative identification of the terms «computer» and «computer», as well as the parallel use of the word «data» («computer data») and the term «computer information».

Among the comments pertaining to article 22 of the Criminal Code of the Republic of Kazakhstan, it is also possible to refer to such wording as «... use or distribution of malicious computer programs and software products» which is usually understood as the cessation of the normal functioning of computer programs and software products. However, the disposition indicates only the informative feature of the broken computer programs and does not indicate similar actions aimed at disrupting the computer operation, or the appearance of any disturbances or disruptions in the «work», a decrease in the operability of individual computer links; arbitrary failure, refusal to issue information or the issuance of distorted information while maintaining the integrity of the computer, the computer system, to activities that interfere with the normal operation of computer equipment (malfunction, reduced efficiency of computers, computer systems or their networks, computer «hang» and others).

Moreover, as some authors point out, the lack of an indication of the degree of disruption of the work of computer programs and software will lead to the fact that for almost any disruption of the work of computer programs and software products (a slight decrease in efficiency (performance or speed), any «hang» of computer programs and software product, any abnormal situation) there is an opportunity to bring to criminal responsibility (VorobYov V.V., 2000: 26; Rogers Marcus K., Seigfried K., 2004:14).

The problem is exacerbated by the fact that, as stressed by scientists, at present there is no complete unification of terminology and deeds recognized as offenses in the field of information and IT technologies (Brenner Susan W., Koops Bert-Jaap, 2004: 18; Banisar D., 2011: 21; Richard A., 2003: 228; Colin B., 1997: 16).

Moreover, the problems are aggravated by the fact that, at the present time, an overwhelming amount of computer equipment, most programs have reached such a high level of complexity, in which the most unpredictable cause can lead to malfunctions in the computer («hang-up, slowdown or performance») (unsuccessful computer configuration, «outdated» drivers, CPU temperature, disconnect between hardware and / or software (from different vendors), programs among themselves (even e and license, from different manufacturers). Therefore, the process becomes uncontrollable, which makes it possible to hold criminally responsible in a similar situation, and this in our view is not entirely permissible.

Conclusion

In our opinion, it is necessary to expand the composition of computer crimes in the Criminal Code of the Republic of Kazakhstan. However, realizing the complexity of the process of introducing new norms into an existing and existing normative legal act, it is possible to propose the adoption of a new law «On the Prevention and Combating Crimes in Global Communication Networks».

Moreover, we can draw the following conclusions:

– offenses in the field of informatization can be considered in a narrow and broad sense, and in the latter case they are understood as any crimes committed using a computer;

– a common moment, uniting all crimes of information character, is the use in the construction of trains of such crimes and terms denoting various information phenomena. Such terms should be used, firstly, correctly from the point of view of information theory, and secondly, uniformly in the entire text of the criminal law. Violation of these requirements will mean non-compliance with such principles of criminalization as the lawlessness of law and the inescapability of the ban, as well as the certainty and unity of terminology.

– the national criminal legislation of the Republic of Kazakhstan lags somewhat behind the leading foreign countries in the prevention and combating of computer crimes in a broad sense, since no such computer crime has been reflected in the text of the criminal law of Kazakhstan;

– computer crimes in the narrow sense, presented in Chapter 7 of the Criminal Code of the Republic of Kazakhstan, are crimes of information character due to the specific nature of their object and the subject of the crime;

– in the current criminal legislation of the Republic of Kazakhstan, there are significant discrepancies with the Convention on Cybercrime with regard to the content of articles on computer crimes, despite the fact that Kazakhstan is a full participant in international relations.

This means that the types of crimes committed through global communication networks have a wide range, which creates certain difficulties in developing measures aimed at preventing and combating this type of crime, the more that the state of the current national criminal law of the Republic of Kazakhstan can not be considered satisfactory and corresponding to the existing reality, since the discrepancy of the Criminal Code of the RK to the norms of the criminal law of the civilized world community, firstly, ignores the s rich experience in fighting computer crime, which is available in Europe and other foreign countries, and, secondly, will not allow to properly cooperate with foreign counterparts in investigating computer crimes, which are often of a transnational nature.

Литература

1 Уголовный кодекс Республики Казахстан от от 16 июля 1997 года № 167-I (с изменениями и дополнениями по состоянию на 03.07.2014 г.) (утратил силу)

2 Тропина Т.Д. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08 / Т.Д. Тропина. – Владивосток, 2005. – 235 с.

3 Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис….. канд. юрид. наук. – Ижевск: Удмуртский государственный университет, 2002. – 189 с

4 Мицкевич А.Ф. Компьютерные преступления: недостатки правового закрепления в УК РФ и возможные пути совершенствования предупреждения средствами уголовного права // Проблемы предупреждения преступности в сфере высоких технологий: Сб. науч. ст. / отв. ред. А.Н. Тарбагаев. – Красноярск, 2004. – С. 19-20.

5 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК. В редакции Закона РК от 28.12.2016 № 36-VI.

6 Конвенция о киберпреступности. Неофициальный перевод на русский язык по изданию: Draft Convention on Cybercrime and Explanatory memorandum related thereto: final activity report – prepared by Committee of Experts on Crime in Cyber space (OC-CY) Submitted to European Committee on Crime Problems (CDPC) at its 50th plenary session (18-22 June 2001). Secretariat Memorandum prepared by the Directorate General of Legal Affairs. – Restricted, CDPC (2001) 2 rev 2. – Strasbourg, 20 June 2001.

7 Foltz C Bryan, Cyberterrorism, computer crime, and reality // Information Management & Computer Security. ABI/INFORM Global. – 2004. – 12, 2/3. – P. 154-253.

8 Марко Герке. Понимание киберпреступности: Руководство для развивающихся стран. – Апрель, 2009. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

9 Dhillon G., Silva L., Backhouse J. Computer crime at CEFORMA: a case study // International Journal of Information Management 24 (2004). P. 551 -561.

10 Скоромников К.С. Расследование преступлений повышенной общественной опасности: пособие для следователя. – М., 2003. – 566 с.

11 Coleman C., Wilde Sapte D. Securing cyberspace new laws and developing strategies // Computer Law & Security Report. – Vol. 19. no. 2. – 2003. – P. 94-102.

12 Ричардсон Р. Хакеры: дьяволы или святые? // Журнал сетевых решений. – 1998. – Т. 4. – С. 108-119.

13 Beardwood John P., Alleyne Andrew C. Canada: Lawful Access Legislation Bill C-74 // A Journal of Information Law and Technology. – 15 April 2006. –P. 62-63.

14 Shinder, Debra L. Scene of the Cybercrime. Computer Forensics Handbook / Debra L. Shinder. Rockland: Syngress, 2003. – 752 p.

15 Shils A. The Torment of Secrecy: The Background & Consequences of American Security Policies. – Chicago, 1956. – 238 p.

16 Ealy, A. New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention. – SANS Institute 2003. – P. 9 [Электронный ресурс]. – Режим доступа: www.cyber-defense.sans.org/resources/papers/gsec/evolution-hack-attacks-general-overview-types-methods-tools-prevention-105082

17 Медведев С.С. Мошенничество в сфере высоких технологий: дис. … канд. юрид. наук: 12.00.08. – Краснодар, 2008 – 210 с.

18 Завидов Б.Д. О понятии мошенничества и его «модификациях» (видоизменениях) в уголовном праве // Право и экономика. – 1998. – № 11. – С. 16-20.

19 Brenner Susan W., Koops Bert-Jaap, Approaches to Cybercrime Jurisdiction // Hie Journal of High Technology Law / Susan W. Brenner, Bert-Jaap Koops. –2004.–P. 17-20.

20 Combating computer crime. – CPC. USA, 1992. – 311 p.

21 Нурпеисова А.К. Уголовно-правовые и криминологические аспекты компьютерной преступности: дис. …. канд. юрид. наук: 12.00.08. – Караганда, 2010. – 167 с.

22 Биебаева А.А. Критерии деления соучастия на формы и проблемы разграничения некоторых форм соучастия // 10 лет Уголовному кодексу и Уголовно-исполнительному кодексу Республики Казахстан: достижения и перспективы: Материалы межд. науч.-практич. конф. – Караганда, 2007. – Т.1. – С. 136-139.

23 Компьютерные технологии в юридической деятельности: Учебно-практическое пособие // Под ред. Н. Полевого, В. Крылова. – М., 1998. – 344 с.

24 Furnell S.M. The problem of categorising cybercrime and cybercriminals // https://www.cscan.org/download/?id=97

25 Kamini Dashora. Cyber Crime in the Society: Problems and Preventions // Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1, 240-259

26 Воробьёв В.В. Преступления в сфере компьютерной информации (Юридическая характеристика составов и квалификация): дис. ... канд. юрид. наук. – Н. Новгород, 2000. – 201 с.

27 Rogers Marcus K., Seigfried K. The future of computer forensics: a needs analysis survey// Computers & Security (2004) no. 23, P. 12-16.

28 Brenner Susan W., Koops Bert-Jaap, Approaches to Cybercrime Jurisdiction // Hie Journal of High Technology Law / Susan W. Brenner, Bert-Jaap Koops. –2004.– P. 17-20.

29 Banisar D. The Right to Information and Privacy: Balancing Rights and Managing Conflicts. – Canada, 2011. – 46 p.

30 Richard A. Glenn.The Right to Privacy? Rights and Liberties under the Law. – ABC-CLIO, 2003 – 399 p.

31 Colin B. The Future of Cyberterrorism // Crime and Justice International. – 1997. – March. – P. 15 – 18.

References

1 Ugolovnyiy Kodeks Respubliki Kazahstan ot 16 iyulya 1997 goda # 167-I (s izmeneniyami i dopolneniyami po sostoyaniyu na 03.07.2014 g.) (utratil silu)

2 Tropina T.D. Kiberprestupnost: ponyatie, sostoyanie, ugolovno- pravovyie meryi borbyi: dis. ... kand. yurid. nauk: 12.00.08 / T.D. Tropina. -Vladivostok, 2005. — 235 s.

3 Brazhnik S.D. Prestupleniya v sfere kompyuternoy informatsii: problemyi zakonodatelnoy tehniki: dis….. kand. yurid. nauk. – Izhevsk: Udmurtskiy gosudarstvennyiy universitet, 2002. – 189 s

4 Mitskevich A.F. Kompyuternyie prestupleniya: nedostatki pravovogo zakrepleniya v UK RF i vozmozhnyie puti sovershenstvovaniya preduprezhdeniya sredstvami ugolovnogo prava // Problemyi predupre¬zhdeniya prestupnosti v sfere vyisokih tehnologiy: Sb. nauch. st. / Otv. red. A.N. Tarbagaev. Krasnoyarsk, 2004. – S. 19-20.

5 Ugolovnyiy kodeks Respubliki Kazahstan ot 3 iyulya 2014 goda # 226-V ZRK. V redaktsii Zakona RK ot 28.12.2016 # 36-VI.

6 Konventsiya o kiberprestupnosti. Neofitsialnyiy perevod na russkiy yazyik po izdaniyu: Draft Convention on Cyber-crime and Explanatory memorandum related thereto: final activity report – prepared by Committee of Experts on Crime in Cyber space (OC-CY) Submitted to European Committee on Crime Problems (CDPC) at its 50th plenary session (18-22 June 2001). Secretariat Memorandum prepared by the Directorate General of Legal Affairs. – Restricted, CDPC (2001) 2 rev 2. – Strasbourg, 20 June 2001.

7 Foltz C Bryan, Cyberterrorism, computer crime, and reality // Information Management & Computer Security. ABI/INFORM Global. – 2004. – 12, 2/3. – P. 154-253.

8 Marko Gerke. Ponimanie kiberprestupnosti: Rukovodstvo dlya razvivayuschihsya stran. – Aprel, 2009. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

9 Dhillon G., Silva L., Backhouse J. Computer crime at CEFORMA: a case study // International Journal of Information Management 24 (2004). P. 551 -561.

10 Skoromnikov K.S. Rassledovanie prestupleniy povyishennoy obschestvennoy opasnosti: posobie dlya sledovatelya. – M., 2003. – 566 s.

11 Coleman C., Wilde Sapte D. Securing cyberspace new laws and developing strategies // Computer Law & Security Report. – Vol. 19. no. 2. – 2003. – P. 94-102.

12 Richardson R. Hakeryi: dyavolyi ili svyatyie? // Zhurnal setevyih resheniy. – 1998. – T. 4. – S. 108-119.

13 Beardwood John P., Alleyne Andrew C. Canada: Lawful Access Legislation Bill C-74 // A Journal of Information Law and Technology. – 15 April 2006. -P. 62-63.

14 Shinder, Debra L. Scene of the Cybercrime. Computer Forensics Handbook / Debra L. Shinder. Rockland: Syngress, 2003. – 752 p.

15 Shils A. The Torment of Secrecy: The Background & Consequences of American Security Policies. – Chicago, 1956. – 238 p.

16 Ealy, A. New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention. – SANS Institute 2003. – R. 9 [Elektronnyiy resurs]. – Rezhim dostupa: www.cyber-defense.sans.org/resources/papers/gsec/evolution-hack-attacks-general-overview-types-methods-tools-prevention-105082

17 Medvedev S.S. Moshennichestvo v sfere vyisokih tehnologiy: dis. … kand. yurid. nauk: 12.00.08. – Krasnodar, 2008 – 210 s.

18 Zavidov B.D. O ponyatii moshennichestva i ego «modifikatsiyah» (vidoizmeneniyah) v ugolovnom prave // Pravo i ekonomika. – 1998. – # 11. – S. 16-20.

19 Brenner Susan W., Koops Bert-Jaap, Approaches to Cybercrime Jurisdiction // Hie Journal of High Technology Law / Susan W. Brenner, Bert-Jaap Koops. -2004.-P. 17-20.

20 Combating computer crime. – CPC. USA, 1992. – 311 p.

21 Nurpeisova A.K. Ugolovno-pravovyie i kriminologicheskie aspektyi kompyuternoy prestupnosti: dis. …. kand. yurid. nauk: 12.00.08. – Karaganda, 2010. – 167 s.

22 Biebaeva A.A. Kriterii deleniya souchastiya na formyi i problemyi razgranicheniya nekotoryih form souchastiya // 10 let Ugolovnomu kodeksu i Ugolovno-ispolnitelnomu kodeksu Respubliki Kazahstan: dostizheniya i perspektivyi: Materialyi mezhd. nauch.-praktich. konf. – Karaganda, 2007. – T.1. – S. 136-139.

23 Kompyuternyie tehnologii v yuridicheskoy deyatelnosti: Uchebno-prakticheskoe posobie // Pod red. N. Polevogo, V. Kryilova. – M., 1998. – 344 s.

24 Furnell S.M. The problem of categorising cybercrime and cybercriminals // https://www.cscan.org/download/?id=97

25 Kamini Dashora. Cyber Crime in the Society: Problems and Preventions // Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1, 240-259

26 VorobYov V.V. Prestupleniya v sfere kompyuternoy informatsii (Yuridicheskaya harakteristika sostavov i kvalifikatsiya): dis. ... kand. yurid. nauk. – N. Novgorod, 2000. – 201 s.

27 Rogers Marcus K., Seigfried K. The future of computer forensics: a needs analysis survey// Computers & Security (2004) no. 23, P. 12-16.

28 Brenner Susan W., Koops Bert-Jaap, Approaches to Cybercrime Jurisdiction // Hie Journal of High Technology Law / Susan W. Brenner, Bert-Jaap Koops. -2004.- P. 17-20.

29 Banisar D. The Right to Information and Privacy: Balancing Rights and Managing Conflicts. – Canada, 2011. – 46 p.

30 Richard A. Glenn.The Right to Privacy? Rights and Liberties under the Law. – ABC-CLIO, 2003 – 399 p.

31 Colin B. The Future of Cyberterrorism // Crime and Justice International. – 1997. – March. – P. 15 – 18.