IRSTI 10.77.51

Tatarinova Lola[1], Svetlana Shankibaeva[2]

[1]PhD in Law, Associate professor of the department «Jurisprudence and international law»,
«Turan» University, Almaty, Kazakhstan, e-mail: dove_2003@mail.ru, tel.: +77071811800
[2]2nd year student of Magistracy. Specialty: «Jurisprudence», Kazakh-Russian International University,
Aktobe, Kazakhstan, e-mail: svetlana.shankibaeva@mail.ru, tel.: +77475125592

PROBLEMS IN DEFINING SUBJECT OF CRIMES COMMITTED THROUGH THE USE OF GLOBAL INFORMATION AND COMMUNICATION NETWORKS

Global communication network so actively implemented in professional and daily life, that imagine the existence of modern man without them is almost impossible, even if it is not an active Internet user.

As with any significant phenomenon of social life, the Internet inevitably becomes a sphere of action of criminal groups and elements. Commercialization of global communication networks, the vast number of users and the growth of services rendered virtual provoke various kinds of illegal behavior.

The problems of combating crimes in the field of computer technologies are largely due to their transboundary nature, when the existing borders between states, the distance between the perpetrator and the victim, the difference in their communication languages are of no importance. In this case, only computer literacy and preparedness are important. It is to solve the problems associated with the subject of cybercrime, our study is devoted to, as there is a need to reduce the age criterion for people who committed offenses in the field of information.

This article contains a number of recommendations of practical significance that will allow improving the current criminal legislation in the field under investigation. The conclusions made in the work can be applied both in the further scientific investigation of offenses in the field of informatization, and with the direct application of norms that provide liability for offenses in the field of informatization.

Key words: crime, cybercrime, information protection, subject, special subject, age, Responsibility.

Татаринова Лола[1], Шанкибаева Светлана[2]
[1]заң ғылымдарының кандидаты, «Тұран» Университетінің
заңтану және халықаралық құқық кафедрасының доценті,
Алматы қ., Қазақстан, e-mail: dove_2003@mail.ru, тел: +7 707 181 1800
[2]құқықтану мамандығы бойынша 2-курс магистранты, Қазақ-Орыс Халықаралық университеті,
Ақтөбе қ., Қазақстан, e-mail: svetlana.shankibaeva@mail.ru, тел.: +7 747 512 5592

Ғаламдық ақпараттық-коммуникациялық желілерді пайдаланумен жасалған қылмыс субъектілерін анықтау мәселелері

Компьютерлік технологияның дамуы жиырмасыншы ғасырдың аяғы мен жиырма бірінші ғасырдың басындағы адамзат өркениетінің нәтижесі болып табылады. Қазіргі уақытта компьютерлік технологияның көмегінсіз толыққанды жұмыс жасайтын бірде-бір сала жоқ, атап айтқанда, жекелеген базалық деректермен жұмыс істеу және бағдарламалармен қамтамасыз ету.

Компьютерлік және ақпараттық технологиялардың кеңінен таралуы компьютерлер арқылы жасалатын қылмыс түрлерінің пайда болуы мен артуына ықпал етті. Мұндай актілердің қылмыстық-құқықтық сипаттамаларына, оларды жасаған адамдарға, қылмысты алдын алу әдіс тәсілдеріне байланысты, сондай-ақ компьютерлік технологиялар саласындағы қылмыспен күрес, тергеу жұмыстарына қатысты объективтік қиындықтар туындайды.

Компьютерлік технологиялар саласында қылмыстарға қарсы күрес мәселелері негізінен олардың трансшекаралық сипатына байланысты, мемлекеттер арасындағы нақты шекаралар, Құқық бұзушы мен жәбірленушіге арасындағы қашықтық, қарым-қатынас, олардың тілдерінде айырмашылық маңызды емес болып табылады. Бұл жағдайда тек компьютерлік сауаттылығы

мен дайындығы болуы маңызды. Киберқылмыс субъектісіне байланысты нақты мәселені шешу осы зерттеу жұмысында қарастырылған. Өйткені, ақпараттандыру саласында қылмыс жасаған адамдардың жас өлшемдерін төмендету қажеттілігінің уақыты келді.

Бұл мақалада зерттеу саласындағы қолданыстағы қылмыстық заңнаманы жетілдіру үшін практикалық маңызы бар бірқатар ұсыныстар берілген. Зерттеу қорытындылары ақпарат саласындағы құқық бұзушылықтар тақырыбын ары қарай ғылыми зерттеуге және ақпарат саласындағы құқық бұзушылық үшін жауапкершілікті қамтамасыз ету нормаларына тікелей пайдалануға болады.

Түйін сөздер: қылмыстылық, киберқылмыстылық, ақпаратты қорғау, субъект, арнайы субъект, жас мөлшері, жауаптылық.

Татаринова Лола[1], Шанкибаева Светлана[2]
[1]кандидат юридических наук, доцент кафедры «Юриспруденция и международное право»
Университета «Туран», г. Алматы, Казахстан, e-mail: dove_2003@mail.ru, тел.: +7 707 181 1800
[2]магистрант 2 курса специальности «Юриспруденция»
Казахско-Российского Международного университета, г. Актобе, Казахстан,
e-mail: svetlana.shankibaeva@mail.ru, тел.: +7 747 512 5592

Проблемы определения субъекта преступлений, совершаемых с использованием глобальных информационно-коммуникационных сетей

Развитие компьютерных технологий представляет собой основу человеческой цивилизации конца двадцатого и начала двадцать первого веков. В настоящее время практически нет ни одной отрасли, способной существовать и полноценно функционировать без компьютерных технологий, в частности, программного обеспечения и различных баз данных.

Широкое распространение компьютерных и информационных технологий привело к появлению и расширению спектра преступлений, совершаемых посредством компьютеров. В этой связи возникают объективные сложности, касающиеся уголовно-правовой характеристики подобных деяний, лиц, совершающих их, а также связанные со способами и методами профилактики, борьбы и расследования преступлений в сфере компьютерных технологий.

Проблемы борьбы с преступлениями в сфере компьютерных технологий во многом обусловлены их трансграничным характером, когда имеющиеся границы между государствами, расстояния между преступником и потерпевшим, разница в их языках общения не имеют никакого значения. В этом случае важность имеют лишь компьютерная грамотность и подготовленность. Именно решению проблем, связанных с субъектом киберпреступлений, посвящено наше исследование, поскольку назрела необходимость снижения возрастного критерия для лиц, совершивших правонарушения в сфере информатизации.

Данная статья содержит ряд рекомендаций практического значения, что позволит усовершенствовать действующее уголовное законодательство в исследуемой области. Выводы, сделанные в работе, могут применяться как при дальнейшем научном исследовании правонарушений в сфере информатизации, так и при непосредственном применении норм, предусматривающих ответственность за правонарушения в сфере информатизации.

Ключевые слова: преступность, киберпреступность, защита информации, субъект, специальный субъект, возраст, ответственность.

Introduction

The practical development of computer technology, the fact that it has become widespread and involved in all spheres of civilized person life and the world community has made appear new types and subtypes of already existing crimes. Such as computer or cyber crimes, namely unauthorized access to computer information and data, creation, use and dissemination of malicious software programs.

Cyber crimes are relatively new types of offences because of the extensive use of computer-based technology in person's life and inadequacies in the present Penal Law of the Republic of Kazakhstan.

In this regard, relevance of the topic is obvious; it also reveals certain problems, primarily related to taking preventive actions and efforts to combat this type of crime, complicated by the controversial issues in defining cyber crimes.

Certainly, defining subject of the crimes in question is one of the main and difficult problems in explaining cyber crimes.

Research methods: analysis, synthesis, induction, deduction, dialectical method, comparative-legal, normative-logical, formal-legal.

Results

From the general theory of criminal law and criminology we know that only a natural person in other words a human being can be subject of a crime [1; 2; 3; 4; 5; 6]. In addition, according to the national criminal legislation of the Republic of Kazakhstan, a person of sound mind who has attained 16 years of age by the time of the commission of a given crime shall be subject of a crime. (Article 15 Section 1 of the Criminal Code of the Republic of Kazakhstan [7]).

Thus, only persons who have the ability to realize the nature of their actions or omissions and who can be in control of their actions, in other words persons of sound mind who have attained 16 years of age can be subjects of a cyber crime

Taking into consideration that cyber crimes are new types of crime, wide range of computer usage, coming down of the user age and active development of computer technology, there is a problem to bring to justice those who commit computer crimes which are outside of the scope of the generally accepted definition of the subject of a crime. Only persons who have attained 16 years of age shall be criminally liable but practice shows that persons under 16 years of age are active users of personal computers and good at computer software that allows them to hack into other users' devices through different networks. We have to admit that their activity has not caused irreparable injury or irreversible damage to the national security, but that does not mean it will last forever.

There are cases when computer geniuses have not attained 14 years of age, but they have the ability to use computers very skillfully for their own purposes [8; 9].

If even the actions of the computer user who has not attained the age required by law shall be illegal, it will not be possible to bring him to justice, but his parents or legal guardians will be held strictly liable.

Thus, the subject of fraud is a natural person of sound mind who has attained 16 years of age. As S. Medvedev marks in his book, «nowadays minimum age of identity formation, together with criminal social identity has come down in comparison with that established by law before. Minimum age of criminal liability for high-tech fraud should be lowered to 14. That is because of the fact that in most cases the subject of high technology-based fraud and the victim do not have direct contact, and criminal attacks are made through the use of global information and communication networks where a person can conceal (or enter fake) information not only about age but also gender, place of residence, occupation etc. «[10, p. 56; 11, c.169]. Often, fraud schemes are rather simple and juveniles move around the Internet quite easily. All this helps them to commit fraud. If their level of consciousness, the ability to be aware of the reality help them behave intelligently and realize the social danger of theft, we believe that persons who have attained 14 years of age are also able to realize the danger of committing fraud in the network.

Taking into consideration all mentioned above, there is a problem of bringing present criminal law of the Republic of Kazakhstan in accordance with the existing realities. Therefore amendments in Criminal Law will help to hold liable those who have committed certain crime covered by Articles of Chapter 7 of the Criminal Code of the Republic of Kazakhstan.

For a more complete disclosure of the problem we have studied the main categories of persons who are the subjects of computer crime or Internet crime.

So, the first group includes persons who carry out unauthorized access to computer information, Part 1 of Article 205 of the Criminal Code of the Republic of Kazakhstan (general subject). They can be described as following: a person of sound mind who has attained 16 years of age; any person who works with IT and network technologies; a person who uses IT and Internet services (authorized user), but has no right to work with a certain category of information or an unauthorized user.

In this regard, we should admit that Part 1 of Article 205 of the Criminal Code of the Republic of Kazakhstan does not stipulate that a person must have a certain position, be engaged in certain activities, or get some certain education. It means theoretically it can be any person under 16 years of age without any special education.

At the same time, such types of crime mostly are committed by persons with relatively high skills, especially when it comes to unauthorized access to computer data system or computer network, since it requires a complex technological and information activities. Therefore, the more complex and sophisticated the way of unauthorized access is, the narrower the range of the alleged perpetrators will be. First of all it can be the technical staff of computer systems or networks, developers of automated systems, their managers, operators, programmers, telecommunication engineers, information security specialists, etc.[12; 13, c.62; 14, c.16; 15, p.16]

In our opinion, age of criminal liability for high-tech crime may be lowered, since more and more often (mostly abroad) such crimes are being committed by minors under the age of criminal liability

(mainly because of hooligan motives and personal ambitions).

It should be admitted that the source of increased danger is the telecommunication network. Currently, however, if a person under 16 years of age commits a computer crime, he will be held liable in accordance with the norms of the Civil Law, as administrative responsibility for such acts is not established in the Republic of Kazakhstan.

The second group includes persons who break into information systems or telecom networks in previous concert or an organized group. This wrongful act is covered by Part 2 of Article 207 of the Criminal Code of the Republic of Kazakhstan. In this case, the number of persons involved in the crime commission can be quite big. In addition, persons suffering from a new kind of mental disorders: «information diseases» or computer phobias can increase the number of potential criminals. Specialized literature indicates that this category of diseases is caused by the systematic information hunger, information overload, wrong speed of getting information, sudden switching from one information process to another, lack of time to get adapted to the information perceived, «information noise». The study of these issues is currently a branch of medicine which is called information medicine. Most workplaces are being equipped with personal computers, in order to improve data processing speed and use time more effectively, therefore many employees feel exposed because of technical stress which causes a computer phobia. That is, computer crimes can be committed by persons who suffer from this type of mental disorder. It is noted that criminal activities of the persons mentioned are mainly aimed at the physical destruction or damage of computers without any criminal intention. It happens because of partial or complete loss of control over their actions [16, p. 34-35; 17, p. 317; 18, p.556; 19, c.137; 20, p.18]. The classification criteria are not always the same, quite a number of such classifications are offered in the legal literature. For example, we propose the following classification:

breakers of the computer using rules: they commit crimes because of lack of knowledge of technology, the desire to get acquainted with the information they are interested in, steal some software program or use computer services for free;

«white collars»: the so-called respectable criminals: accountants, treasurers, financial managers of different companies. They are characterized by: use of computers to simulate the crime they plan to commit, computer blackmailing of competitors, falsification of information, etc. The purpose of their action is to obtain material benefits or conceal other crimes;

«computer spies,» well-trained technical specialists; their purpose is to get strategic information from different areas;

hackers («obsessed programmers»): the most technically and professionally trained individuals, good at computer science and programming. Their activities are aimed at unauthorized entry into computer systems, theft, modification or destruction of data stored in them. Often they commit crimes without having an intention to obtain direct tangible benefits [21, p. 234; 22, p.154; 23, p.19].

Discussion

With the advent of the first computer crimes, such a group of criminals as hackers appeared.

The English word hacker speaks for itself (the one who hacks, cracks, cuts). Initially this name was given to programmers who preferred not to deal with already installed software on a new computer but delete («knock») everything and install programs they want. Gradually, the term has spread to all the computer fanatics and among them there appeared a classification, i.e. hackers are divided into several groups depending on the activity they have:

1. crackers: the ones who crack computer software. They crack program security to get material benefit. This is the largest group of hackers, and the damage from their activity is measured in millions of dollars. Crackers are the most dangerous enemies for commercial software. If they have an interest in breaking some software, sooner or later hacking will be done, despite the security complexity. Usual «working tool» of crackers is a cracking program which helps an attacker gain access on the system.

2. Phreakers: people who prefer alternative television and other communication services payment. Mainly they fraud PBX: free long-distance calls; if there is a party line they make to pay the other subscriber for their telephone services etc. Phreakers also use the so-called «boxes» special electronic devices that perform various functions. For example, «color boxes» allow you to control the traffic light signals or allow you not to pay for the made calls on touch-tone phones etc. However, according to the criminal law not every act of phreaking is a computer crime, for example, unauthorized connection to subscriber's phone line in order to make free calls cannot be defined as computer crime. This group of crimes is covered by Article 213 of the Criminal Code of the Republic of Kazakhstan. «Unauthorized modification of the

identification code of subscriber mobile device, modification of subscriber identification device, as well as the creation, use and dissemination of programs for changing identification code of the subscriber device», or if there are necessary evidence of such actions, all these are considered to be usual fraud and unfortunately very difficult to prove.

3. Carders pay their expenses with other people's credit cards. This group of hackers is not so big because one needs deep knowledge in the field of radio electronics and circuits programming to succeed in «carding». But at the same time it is one of the most complicated methods of fraud, divided into: «stuff carding», «adult», money-laundering through remittance services. It should be noted that other types of carding may also appear.

4. Network hackers, in other sources «information travelers». This type of phreakers appeared in connection with the development of network technology. Internet provider services were quite expensive, so many computer scientists tried to gain unauthorized access using «holes» in software technologies. Among the network hackers, there are selfless highly qualified people, and those who sell their work for money [24, p. 108-109].

Conclusion

Depending on the goals, objectives and modus operandi, hackers can be divided into: non-criminal and criminal hackers, and in each of the above mentioned groups the following classification is possible:

1. Amateur hackers who as a rule have not attained 15 years of age and want to achieve one of three goals: gaining access to the system to find out its purpose; gaining access to gaming programs; modify or delete the data, as well as leaving a mark, for example an obscene or insulting note. Their motivations to gain access to the system may be different: they vary from the desire to experience the emotional lift when you play with the computer to the feeling of power over the hated boss (provider, etc...). These types of activities can be done by professional programmers as well amateurs. A significant number of perpetrators are gamers, usually between the ages of 15 and sometimes even 12 and 25. However, some of them start not only to look through the information, but also take an interest in the contents of the files, and this is a serious threat, because in this case it is difficult to distinguish between harmless mischief and intentional act [14, p.68].

2. Qualified hackers who perfectly know computing and communication system spend a lot of time on thinking about the ways how to break into systems and even more time on experimenting with those systems. Their goal is to identify and overcome the security system, to explore the possibilities of computer and after achieving the goal leave with satisfaction.

These people have high qualification and realize that the level of risk is low, as they do not have motives of destruction or theft.

The category of criminal professionals typically include: criminal groups that pursue political goals; individuals seeking to obtain information for the purpose of industrial espionage, and, finally, the groups of individuals who seek profit. Professional hackers try to minimize the risk, so they look for and involve in their actions working or recently resigned employees of the target company because the risk of being detected trying to entry in banking system from outside is rather high.

As for the age of these persons in the legal literature there are different age limits: basically not higher than 30-35. At the same time it is believed that between 15 and 25 years of age hacker is not rich and unselfish and starting with 30-35 years of age begins to look for ways of illegal enrichment [25, p. 348; 26, p.672; 27, p.284; 28; 29, p.215; 30].

Thus, based on our studies, we should admit the fact that current criminal laws of the Republic of Kazakhstan in combating computer crime do not correspond to present realities and need to be improved.

Firstly, the definition of subject of high-tech crimes should be amended. In our opinion, subject of crime should be defined as a person of sound mind who has attained 14 years of age.

At the same time there are several categories of subjects of the crime:

1) persons who carry out unauthorized access to computer information, Part 1 of Article 205 of the Criminal Code of the Republic of Kazakhstan (general subject);

2) group of persons who carry out unauthorized access to computer information in previous concert or an organized group – Part 2 of Article 207 of the Criminal Code of the Republic of Kazakhstan;

3) persons who create, use and disseminate malicious computer programs and software abusing official position, – Part 2 of Article 210 of the Criminal Code of the Republic of Kazakhstan.

Secondly, it is appropriate to amend Part 2 of Article 15 of the Criminal Code of the Republic of Kazakhstan: «Persons who have attained 14 years of age by the time of the commission of a crime shall

be criminally liable ... .for unauthorized access to computer information, creation, use and dissemination of malicious computer programs (Chapter 7 of the Criminal Code of the Republic of Kazakhstan).»

In summary, it is important to note that number of issues discussed in this Article concerning main types of crimes committed through the use of global information and communication network, as well as number of problems in defining the subject of such crimes is rather big, and we have tried to analyze them from the position that helps to define types and subjects of all categories of computer crimes. However, each type and subtype of computer crimes committed through the use of the global information and communication network, has its own specific features, which will be discussed in more detail in subsequent sections of this monographic work.

Литература

1 Диаконов В.В. Уголовное право России (Общая часть): учебное пособие. – М., 2003. // Все о праве [Электронный ресурс]. – Режим доступа: http://www.allpravo.ru/library/doc101p/instrum104/

2 Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. … канд. юрид. наук: 12.00.08. – М., 2006. – 186 с.

3 Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: автореф. дис. … канд. юрид. наук: 12.00.08. – М., 1998. – 24 с.

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

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

6 Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дисс. …канд. юрид. наук. – Красноярск: Красноярский ГУ, 2002 – 202 с.

7 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК // Ведомости Парламента РК. – 2014. – № 13-II. – Ст. 83.

8 Самый молодой в мире сисадмин – девятилетний мальчик! // dondass UA [Электронный ресурс]. – Режим доступа: http://donbass.ua/news/technology/2010/01/22/samyi-molodoi-v-mire-sisadmin-devjatiletnii-malchik.html

9 В Турции задержан самый молодой хакер // Vesti.az [Электронный ресурс]. – Режим доступа: http://vesti.az/news/9835

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

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

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

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

15 Rogers Marcus K., Seigfried K. The future of computer forensics: a needs analysis survey// Computers & Security (2004) 23, 12-16.

16 Вехов В.Б. Компьютерные преступления: способы совершения, методы расследования. – М., 1996. – 296 с.

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

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

19 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.

20 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.

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

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

23 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.

24 Ричардсон Р. Хакеры: дьяволы или святые? // Журнал сетевых решений. – 1998. – Т. 4. – С. 108-109.

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

26 Chung W., Chen H., Chang W., Chou Sh. Fighting cybercrime: a review and the Taiwan experience // Decision Support Systems, Volume 41, Issue 3, March 2006, Pages 669-682.

27 Wiemans F.P.E. Onderzoek van gegevens in geautomatiseerde werken. -Nijmegen: Wolf Legal Publishers, 2004. 284 p.

28 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

29 Ral Rojas, Ulf Hashagen, Raul Rojas. Regarding the development of computer systems, see Hashagen, The first Computers – History and Architectures. – The MIT Press, 2000. – 471 p.

30 Problems of criminal procedural law connected with information technology. Council of Europe Publishing. – 1996.

References

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

2 Biebaeva A.A. Kriterii (2207) deleniya souchastiya na formy i problemy razgranicheniya nekotoryh form souchastiya // 10 let Ugolovnomu kodeksu i Ugolovno-ispolnitel'nomu kodeksu Respubliki Kazahstan: dostizheniya i perspektivy: Materialy mezhd. nauch.-praktich. konf. – Karaganda, 2007. – T.1. – S. 136-139. (Criteria for the division of complicity into forms and problems of distinguishing certain forms of complicity).

3 Brazhnik S.D. (2002) Prestupleniya v sfere komp'yuternoy informacii: problemy zakonodatel'noy tehniki: dis….. kand. yurid. nauk. – Izhevsk: Udmurtskiy gosudarstvennyy universitet,– 189 s. (Crimes in the field of computer information: problems of legislative machinery).

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

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

6 Chung W., Chen H., Chang W., Chou Sh. (2006) Fighting cybercrime: a review and the Taiwan experience // Decision Support Systems, Volume 41, Issue 3, Pages 669-682.

7 Coleman C., (2003) Wilde Sapte D. Securing cyberspace new laws and developing strategies // Computer Law & Security Report. – Vol. 19. no. 2.

8 Combating computer crime.(1992) – SRS. USA, – 311 r.

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

10 Diakonov V.V. (2003) Ugolovnoe pravo Rossii (Obshhaya chast'): uchebnoe posobie. – M., 2003. // Vse o prave [Elektronnyy resurs]. – Rezhim dostupa: http://www.allpravo.ru/library/doc101p/instrum104/ (The Criminal Law of Russia (General part)).

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

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

13 Karpov V.S. (2002) Ugolovnaya otvetstvennost' za prestupleniya v sfere komp'yuternoy informacii: diss. …kand. yurid. nauk. – Krasnoyarsk: Krasnoyarskiy GU, 202 s. (Criminal liability for crimes in the field of computer information).

14 Komp'yuternye tehnologii v yuridicheskoy deyatel'nosti: Uchebno-prakticheskoe posobie // Pod red. N. Polevogo, V. Krylova. – M., 1998. – 344 s. (Computer technologies in legal activity).

15 Malykovcev M.M. (2006) Ugolovnaya otvetstvennost' za sozdanie, ispol'zovanie i rasprostranenie vredonosnyh programm dlya EVM: dis. … kand. yurid. nauk: 12.00.08. – M., 2006. – 186 s. (Criminal liability for the creation, use and distribution of malware for computers).

16 Medvedev S.S. (2008) Moshennichestvo v sfere vysokih tehnologiy: dis. … kand. yurid. nauk: 12.00.08. – Krasnodar, – 210 s. (Fraud in the sphere of high technologies).

17 Nurpeisova A.K. (2010) Ugolovno-pravovye i kriminologicheskie aspekty komp'yuternoy prestupnosti: dis. …. kand. yurid. nauk: 12.00.08. – Karaganda, – 167 s. (Criminally-legal and criminological aspects of computer criminality).

18 Problems of criminal procedural law connected with information technology. Council of Europe Publishing. – 1996.

19 Ral Rojas, Ulf Hashagen, Raul Rojas. (2000). Regarding the development of computer systems, see Hashagen, The first Computers – History and Architectures. – The MIT Press, 2000. – 471 r.

20 Richardson R. (1998) Hakery: d'yavoly ili svyatye? // ZHurnal setevyh resheniy. – T. 4. – S. 108-109. (Hackers: devils or saints?).

21 Rogers Marcus K., Seigfried K. (2004) The future of computer forensics: a needs analysis survey// Computers & Security 23, 12-16.

22 Samyy molodoy v mire sisadmin – devyatiletniy mal'chik! // dondass UA [Elektronnyy resurs]. – Rezhim dostupa: http://donbass.ua/news/technology/2010/01/22/samyi-molodoi-v-mire-sisadmin-devjatiletnii-malchik.html (The youngest sysadmin in the world is a nine-year-old boy).

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

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

25 Skoromnikov K.S. (2003) Rassledovanie prestupleniy povyshennoy obshhestvennoy opasnosti: posobie dlya sledovatelya. – M.,– 566 s. (Investigation of crimes of increased social danger).

26 Smirnova T.G. (1998) Ugolovno-pravovaya bor'ba s prestupleniyami v sfere komp'yuternoy informacii: avtoref. dis. … kand. yurid. nauk: 12.00.08. – M.,. 24 s. (Criminally-legal struggle against crimes in the field of the computer information).

27 Ugolovnyy kodeks Respubliki Kazahstan ot 3 iyulya 2014 goda № 226-V ZRK // Vedomosti Parlamenta RK. – № 13-II. – St. 83. (The Criminal Code of the Republic of Kazakhstan).

28 V Turcii zaderzhan samyy molodoy haker // Vesti.az [Elektronnyy resurs]. – Rezhim dostupa: http://vesti.az/news/9835 (The youngest hacker detained in Turkey).

29 Vehov V.B. (1996) Komp'yuternye prestupleniya: sposoby sovershenіya, metody rassledovaniya. – M., 1996. – 296 s. (Computer crimes: ways of committing, methods of investigation).

30 Wiemans F.P.E. (2004) Onderzoek van gegevens in geautomatiseerde werken. -Nijmegen: Wolf Legal Publishers, 284 p.