COMPUTER CRIMES

Nurabay Arailym Taishibaykizi, the 2nd course of International Law, ENU.
Supervisor: PhD in Law, docent Gasanov A.A.

Computer crimes are any illegal actions at which the computer acts or as object against which the crime is done or as a tool that is used for fulfilment of criminal acts. There are wide range of actions which can be divided into four categories concerning computer crimes: theft of the computer equipment; a computer piracy (illegal activity in software sphere); not authorised access to computer system with a view of damage or information destruction; use of the computer for fulfilment of illegal or roguish actions. As computer systems receive more and more a wide circulation, and business circles in the increasing degree rely on computers and often store on them the confidential information, criminals find more and more ways of use of computers for fulfilment of illegal actions.[7]

World practice shows, that the damage from computer crimes can be estimated in the sums making annual budgets of large cities. In the majority of the countries of Europe and America the computer criminality gives incomes, comparable with the incomes received from a drug trafficking and the weapon.[8] The British government has calculated how much costs the economy cybercrime. It is estimated by the British Government, that the amount of damage from computer crime is 43 billion dollars a year - about 2% of the proceeds of economic production of the country. Thus, conclude in the UK, criminals still get a huge profit at the expense of state funds and private business. Therefore, computer crimes are directly related, to the criminal as well as to the economic crimes.

One type of computer crime known as "hacking" (a term that refers to the unauthorized entry into a computer system). To gain access to "secure" computer system or network, the user must have a password. Hackers use a variety of ways to recognize the secret passwords, or bypass the password protection system. The possibility of invasion of computers into telephone networks and through a complicated way interconnected computer systems, without leaving fingerprints or traces, substantially complicates the identification and apprehension of hackers. Once "inside" the computer system, the hacker can change, delete or copy the data stored in the network. A hacker can gather confidential personal and financial information about companies and individuals, and then use it for extortion or by bank fraud. It can intercept information transmitted over communications lines, copy the data transmitted over the Internet, record credit card numbers and personal passwords. A hacker can introduce a system of program codes or modify existing ones, resulting in computers will execute the commands of the attacker. In 1996, was committed by unauthorized access to computer systems website of the Ministry of Justice. Attackers have destroyed the contents of over 200 catalogs and posted a page with a picture of Adolf Hitler, swastikas, scenes of a pornographic nature and others of this kind.[9]

Hackers, writing computer viruses, are arrested, prosecuted and punished for crimes they committed. Usually, the viral program is embedded into another innocuous program, such as a

[7] Online encyclopaedia Krugosvet
[8] Criminal law. Special part. Textbook. A.S. Mihlina, Moscow.: Urisprudenciya, 2000.-200page
[9] http://www.crime-research.ru/news/07.02.2007/3210/

utility for text processing, which can be obtained free of charge from the Internet or from any other computer system with an electronic bulletin board.[10]

Like many revolutionary technology - computer technologies have great potential for both progress and abuse. Attacks on the network, fraud, software piracy, electronic espionage, child pornography, theft of funds from bank accounts - are just some of the crimes committed using computer systems.[11]

National infrastructure of any country is closely connected with the use of modern computer technology. Daily banking and energy systems, air traffic control, transportation network, even the ambulance are at the mercy of safe and reliable operation of automated computing systems.[12]

In Kazakhstan, the jurists have long ago started to raise the question of need of consolidation of legal relations arising from the different applications of automatic information processes. Definite step towards realization of these wishes was the adoption of the Civil Code in 1995, which contains several provisions related to the protection of information: "Civil law protects the information that constitutes proprietary or trade secret, in the case where information has an actual or potential commercial value by virtue of unknown to third parties, for there is no free access to the lawful owner of the information and take measures to protect its confidentiality."(p. 1 of article 126 of Civil Code). As well as the development of the Criminal Code 1997 (with subsequent correction in 2002) article, there were stated grounds of criminal liability for so-called computer crime. Government of the Republic of Kazakhstan from August 16, 2002, for consideration by Members of Parliament presented the draft law "On informatization".

As part of Article 227 of the Criminal Code, computer information in each case is only the subject of the commission of computer crime. However, when using the machine information as means of committing another crime, it is also related to its protection, it will inevitably suffer, i.e, it becomes an object of socially dangerous act. It is impossible to illegally use the information stored in the computer, without violating its protection, i.e without committing one of the acts listed in article 20 of the Law "On Informatization": leakage, loss, distortion, falsification, destruction, modification, copying, locking, and other forms of unlawful interference with information resources and systems, violation of privacy (Article 142 of the Criminal Code), as well as breach of copyright and related rights (Article 184 of the Criminal Code), illegal receipt and disclosure of information constituting a commercial or banking secret (Art. 200 CC).

In chapter 7 of the Criminal Code, "Crimes in the sphere of economic activity" in article 227 identifies the following socially dangerous acts by means other computer equipment. Unauthorized access to the records of computer programs, to primary documents, databases and such other information, made as a record by a human hand, typewritten, or printer, typed hard copy, not implied in the rules of criminal law, and may, in appropriate cases, result in liability only other article of the Criminal Code (Art. 175, 177, 180, 184 and others).

According to employees of the Home Office of Kazakhstan, established in April 2003, which is competent organization works to identify, disrupt and disclosure cybercrimes and crimes committed with the use of high technology, the number of crimes involving computer technology and information technology is growing. So, if in 2003 the internal affairs authorities had registered 17 crimes and offenses in this category, in 2004 - 26, 2005 - 713, and number of registered similar cases in 2006 were 1437. However, experience shows that law enforcement becomes aware of computer crimes not more than about 5-10% of all committed computer crimes. In the Republic of Kazakhstan in recent years, there was not a single crime under

[10] Online encyclopaedia Krugosvet
[11] Douglas Hayward.The dark side of hacking became darker. // www.connectex.kiev.ua
[12] Golubev V.A. Interview: Computer crime – threats and forecasts. - http://www.crime-research.ru/interviews/golubev_interv06/

article 227 of the Criminal Code (illegal access to computer information, the creation, use and dissemination of malicious software) it is clear demonstration of latency of this type of crime.

The criminalization of computer crime - necessary but insufficient condition for effective control. Along with the criminal, civil, administrative and legal protection of computer software an essential element in the eradication of such violations was the establishment in some countries, special units (within the law enforcement agencies) to combat computer crime.

In Portugal, for example, in 1991 was adopted a law 109/91 on Cybercrime. Article 5 of the Act states, that the intentional infliction of damage to computer data is punishable by fine or imprisonment for a term of 3 to 10 years depending on the severity of the crime. Attempts to commit crime are also punishable. Article 6 provides liability for computer sabotage - an illegal alteration, destruction, suppression of data or programs, or interference with the system by other means in order to prevent system performance or breach of its functioning. Person, who committed this crime, faces a fine or imprisonment for up to 5 years. If the offense caused serious damage, the penalty may be imposed only in the form of imprisonment for a term of 1 to 5 years. The act also provides penalties for unauthorized access- to the system without the right, with the intention of obtaining illegal profit or advantage for himself or a third person. Attempt to commit crime is also punishable. Sanction for that is fine or imprisonment for up to 3 years if the access occurred, breaking the security measures, and imprisonment for up to 5 years, when access was aimed at obtaining industrial or commercial secrets protected by law, and the goal of obtaining a large economic benefits . And finally, Article 8 of the Act is devoted to the illegal interception of telecommunications, the use of technical devices within a communications system, or within the network. Attempt to this crime is also punishable. For committing a crime punishable - a fine or imprisonment for up to 3 years.

In conclusion I would like to acknowledge some of the main directions of development of legislation to fight computer crimes.

1. We need to ensure that the legal regulation of the spread of mass media, posting on Internet sites, including, ensuring implementation of the constitutional ban on propaganda or agitation instigating social, racial, ethnic and religious strife, the proliferation of pornographic and other information, as well as secure the obligation of public authorities to protect official information available on their websites.

2. Improving the criminal procedure law shall establish conditions to law enforcement authorities promptly and effectively in cases of threats to the security implemented by using information and communication technologies, uniform issue of evidence obtained through computer systems and telecommunications.

3. Legislation in the field of communication also requires improvement in several respects. It should ensure that:

• Disclosure of the competent authorities of sufficient data on the flow of information to identify service providers and routes of transmission of information

• Online service provider for communication of information about the subscribers (type and time of services rendered, the user's identity, address, phone number, payment details and other information) are not associated with the content they transmit information.

• We should make new articles of the Criminal Code relating to different types of computer crimes and punishments for them. We must take into consideration the experience of foreign countries, for example, we can apply the methods of punishment of crimes used in the Criminal Code of Portugal.

4. There is a necessity of removing the legal uncertainty regarding the use of employers of visual observation, means of control of telephone calls, emails, use of Internet access, since these funds can be used for illegal activities.

5. There should be no anonymity in certain areas of the Internet, because it involves a lot of negative consequences, and its borders will have to be objectively narrowed.

6. Also, the objective problem is the newness of the scope of legal regulation, the lack of an established theoretical framework for the development of legislation. In particular, it is not

defined legal content of the basic concepts. Because knowledge is the cornerstone for a beginning that should be given properly to IT professionals in order to enable them to block all malicious intrusions, and to provide safe protection.

References:

1. The Constitution of the Republic of Kazakhstan, 1995
2. The Criminal Code of the Republic of Kazakhstan dated 16 July 1997
3. The Civil Code of the Republic of Kazakhstan dated March 23, 1995 (General)
4. The Civil Code of the Republic of Kazakhstan from July 1, 1999 (special part)
5. Law of the Republic of Kazakhstan dated 08.05.2003 N 412-2 "On Informatization"
6. Online Encyclopedia Krugosvet
7. "Criminal Law. Special part. "AS Mikhlina, Moscow, 2000
8. www.connectex.kiev.ua
9. RF Law "On Legal Protection of Computer Programs for electronic computers and databases of 23 September 1992
10. Simkin, L. How to stop piracy, Russian justice .- 1996
11. crime-research.ru