IRSTI 10.77.51

Yergali A.M.[1], Amangeldi B.S.[2]

[1]Ph.D, e-mail: yergali.adlet@gmail.com
[2] Master of 1-course, Law Faculty
Al-Farabi Kazakh National University, Kazakhstan, Almaty

PROBLEMS OF COUNTERACTION OF CRIME IN THE SPHERE OF INFORMATION TECHNOLOGIES

With the growth in the volume of use of computer technologies and their significance in the lives of people in the world, a new type of crime in the field of information technology has appeared. The article is devoted to a detailed analysis of the emergence of crime in the field of information technology, as well as methods to combat this crime. The author reveals the rapid development for a short time of this type of crime in the field of information technology on the basis of a comparative analysis of the Republic of Kazakhstan with other countries. Special attention was paid by the author to stimulating factors to the emergence and consistent growth of crime in the field of information technology. The article problems of counteraction of crime in the sphere of information technologies are considered.

The author comes to the greatest public danger is constituted by the crimes connected with illegal access to computer information. And also, on the basis of a comparative analysis of the Republic of Kazakhstan and other countries, the origin of this type of crime will be explained.

Key words: crime, counteraction, information technologies, computer, information communications.

Ергали А.М.[1], Амангельды Б.С.[2]

[1]PhD, e-mail: yergali.adlet@gmail.com
[2]заң факультетінің 1 курс магистрі
әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан, Алматы қ.

Ақпараттық технологиялар саласындағы қылмыстылыққа қарсы тұру мәселелері

Компьютерлік технологияларды пайдалану көлемінің өсуі мен олардың әлемдегі адамдардың өміріндегі маңыздылығының артуының нәтижесінде ақпараттық технологиялар саласындағы қылмыстардың жаңа түрі пайда болды. Мақала ақпараттық технологиялар саласындағы қылмыстардың пайда болуы мен осы қылмыстарға қарсы күрес әдістеріне жан-жақты талдау жасалып қарастырылған. Автор Қазақстан Республикасының басқа мемлекеттермен салыстырмалы талдауының негізінде ақпараттық технология саласындағы қылмыстардың қысқа уақыт ішінде жылдам дамуын айқындайды. Автор ақпараттық технология саласындағы қылмыстардың пайда болуы мен дәйекті өсуіне ықпал ететін факторларға ерекше назар аударды. Сондай-ақ, мақалада ақпараттық технологиялар саласындағы қылмыстылыққа қарсы тұру мәселелері қарастырылды.

Автор компьютерлік ақпараттарға заңсыз қол жеткізуімен байланысты қылмыстық құқық бұзушылықтар аса қоғамдық қауіп төндіреді деп тұжырымдайды. Сондай-ақ, Қазақстан Республикасының басқа мемлекеттермен салыстырмалы талдауының негізінде мұндай қылмыстың туындау себептерін айқындайды.

Түйін сөздер: қылмыстылық, қарсы тұру, ақпараттық технологиялар, компьютер, ақпараттық байланыс.

Ергали А.М.[1], Амангельды Б.С.[2]

[1]доктор PhD, e-mail: yergali.adlet@gmail.com
[2]магистрант 1 курса юридического факультета
Казахский национальный университет им. аль-Фараби, Казахстан, г. Алматы

Проблемы противодействия преступности в сфере информационных технологий

С ростом обьема использования компьютерных технологий и их значимости в жизни людей в мире появился новый вид преступности в сфере информационных технологий. Статья посвещена детальному анализу появления преступности в сфере информационных технологий, а также методам борьбы с этой преступностью. Автор раскрывает слишком быстрое развитие за малое время этого вида преступности в сфере информационных технологий на основе сравнительного анализа Республики Казахстан с другими странами. Особое внимание обращено автором на стимулирующие факторы появления и последовательному росту преступности в сфере информационных технологий. В статье также рассмотрены проблемы противодействия преступности в сфере информационных технологий.

Автор приходит к выводу, что наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. А также поветствует на основе сравнительного анализа Республики Казахстан с другими странами причины возникновения этого вида престпуности.

Ключевые слова: преступность, противодействие, информационные технологии, компьютер, информационные связи.

Growth of volumes of information, computer networks and number of users, simplification of their access to information circulating on networks significantly increases probability of plunder or destruction of this information.

Now the importance of a problem of protection of information resources, including personal, is defined by the following factors:

- development of the world and national computer networks and new technologies providing access to information resources;
- transfer of information resources to electronic media and their concentration in information systems;
- increase in «price» of the created and saved up information serving as a real resource of welfare and personal development;
- development and improvement of information technologies which can effectively be used by criminal structures.

Computer crime became the real scourge of economy of the developed states. So, for example, 90% of firms and the organizations in Great Britain at different times became objects of electronic piracy or were under its threat(Security Gazette, 1980: p.7), in the Netherlands 20 different % of the enterprises(Computer Law and Security, 1991: p.2-3) became the victims of computer crime. In Germany with use of computers 4 billion euros, and in France – 1 billion euros are annually abducted(Selivanov, 1993: p.36).

The greatest public danger is constituted by the crimes connected to illegal access to computer information. It is known, the considered offense has very high latency which according to different data makes 85-90%(Vekhov, 1996: p.44). Moreover, the facts of detection of illegal access to information resources for 90% have accidental character(Baturin, 1991: p.134).

Crime of this look as the world practice shows, does huge material and moral harm. So, for example, annual losses only of a business sector of the USA from unauthorized penetration into information databases make from 150 to 300 billion dollars(Lapshin, 1997: p.107).

In modern conditions of social and economic development of the Republic of Kazakhstan computer crime has become a reality of public life.

Dynamics and scales of computer crimes are shown clearly by the following data . For the last ten years their number has increased by 22,3 times and continues to grow on average by 3,5 times annually. The annual extent of material damage from these criminal encroachments is 613,7 million rubles. The average damage caused to the victim from one computer crime is equal to 1,7 million rubles. With a certain share of success only about 49% of crimes are investigated, convictions are pronounced only in 25,5% of cases of total number of the brought criminal cases. The average value – number of criminal cases on which production is suspended makes 43,5% and brightly reflects low degree of professionalism of law enforcement officers in activities for disclosure, investigation and prevention of these criminal encroachments(Starostina, 2005: p.89).

The analysis of problems of fight against computer crime allows to draw a conclusion that her emergence and consecutive growth is promoted by a number of factors: political, social, economic and legal. So, 87% of the interviewed respondents consider that economic factors have significant effect on emergence and development of computer crimes, 35% - mark out social factors, 30% - legal and only 13% - political. At the same time 92% of respondents are sure that in process of a computerization of the Russian society the number of computer crimes will increase. The following has been distinguished from the sectors of national economy having now optimum conditions for commission of computer crimes: mixed (33% of respondents), state (32% of respondents), in all equally (31% of respondents), and among branches economies are bank (81%) and financial (53%) (threats and forecasts//www.crime-research.ru).

The following main tendencies of development of computer crime in Kazakhstan are allocated (Lopatina, 2006: p.16): a) the highest growth rates; b) mercenary motivation of the majority of the committed computer crimes; c) complication of ways of commission of computer crimes and emergence of new types of illegal activity in the sphere of computer information; d) growth of criminal professionalism of computer criminals; e) rejuvenescence of computer criminals and increase in a share of the persons who were earlier not brought to trial; e) growth of material damage from computer crimes in the general share of damage from other types of crimes; g) transfer of the center of gravity on commission of computer crimes with use of computer networks; h) development of computer crime into the category of transnational crime; i) high level of latency of computer crimes.

Why computer crimes are committed? It is impossible to answer unambiguously. It and complexity in search of traces of criminals, and latency. So chances to be caught at the computer criminal much less, than at the robber of bank, even at capture he has less chances to get to prison. 1% of computer crimes is found on average. And the probability that for computer fraud will get to prison is less than 10%(Dulov, 1973: p.168). It is possible to carry to the reasons or motives for which crimes in the field of computer information are committed: self-interest, hooligan motives, revenge, computer espionage and diversion, self-expression, accident, vandalism.

There is also the following classification, in a percentage ratio mercenary reasons (66%), political goals (17%), research interest (7%), hooligan motives and mischief (5%), revenge (5%).

And the most typical criminal intents are:

- forgery of accounts and pay-sheets;
- addition of overhours;
- falsification of payment documents;
- plunder of cash and non-cash money;
- secondary receiving already made payments;
- transfer of money to fictitious accounts;
- money laundering;
- money laundering;
- shopping with fictitious payment;
- illegal currency transactions;
- illegal receiving credits;
- manipulations with the real estate;
- receiving illegal privileges and services;
- sale of confidential information;
- plunder of material values, goods, etc.

At the same time, as a rule, with plunder of money 52% of crimes, are connected with destruction and destruction of means of the computer equipment – 16%, with substitution of basic data – 12%, with plunder of information and programs and also with plunder of services – 10% (Research Centers of the All-Russian Research Institute of the Ministry of Internal Affairs of the Russian Federation, 2012: p. 2-3).

On official statistics, in the USA the computer crimes committed by employees make 70-80% of the annual damage connected with computers. Other 20% are actions of dishonest and dissatisfied employees and they are made for a number of reasons(Goben, 1994: p. 215-248).

The greatest danger is constituted by persons from among permanent members of staff – system programmers, network administrators, specialists in information security, operators of the COMPUTER, engineering personnel and also users of system.

The competitors or persons who are engaged industrial in espionage and also professional criminals and cyberterrorists can put serious threat of network safety. Representatives of these groups carry out illegal activity in the wide range from corporate espionage before extremely dangerous diversions against computing systems of the vital objects (Osipenko, 2004: p.152).

In recent years researchers of the identity of the criminal on the wide computer networks faced essential extension of criminal activities from hackers. On a level of potential danger from this or that category of criminals of FBI of the USA predict probable sources of security risks of wide area networks

It is not so simple to find the solution against a spam. After all, a spam is a business which makes huge profit for those who use it. Distributors of a spam permanently enhance technologies of remote access and are not going to give up without fight. Noticeably to reduce quantity of unwanted mail, radical reconstruction of all electronic mail system is necessary.

Analyzing structure of internal threats, experts mark as the most serious systems of the actions from the point of view of violation in information security field taking place in the last two years, such negative manifestations of a human factor in operation of a staff as unwarranted installation and use of the independent software (to 78% of internal incidents), increase in cases of use of the equipment and resources for personal reasons (for 10%). Lowering for 7% of quantity of the cases connected to installation and use of the independent equipment owing to toughening of monitoring from administration is at the same time marked.

Even in the Pentagon serious violations of rules of information security which are shown that practice of not considered programs and programs with expired certificates is widespread take place. According to experts, existence of a large number (288) software products which don't have necessary certificates and employees, responsible for their operation, poses in itself potential threat for safety not only military, but also national infrastructure in general.

Organized criminal communities even more often use possibilities of the Internet for commission of fraud in the credit and financial sphere and electronic trading system.

Specialists of Symantec and Message Labs in one of the last reports note that hackers carry out harder and harder attacks already not for fun, and for the purpose of enrichment. The most attacked in the recent past were the websites of electronic commerce. 16% of all attacks were the share of them that there is 400% above than the level of first half of 2004 when it has made 4%. Similar growth shows change of reference points of hackers. If earlier they dreamed only of glory, then now personal enrichment becomes a priority.

According to National Separation of FBI on computer crimes, from 85% to 97% of attacks on corporate networks not that are not locked, but also are not found. The tests which are carried out to the USA showed the following results: in 88% of cases penetration of special groups of experts into military information systems was successful, in 4,36% of cases of the attack were found, and only in 5% system administrators reported about such attacks. Other group of experts inspected about 8 thousand computers of the U.S. Department of Defense and found 150 thousand weak spots.

The number of the crimes committed in a cyberspace grows in proportion to number of users of computer networks, and, by estimates of the Interpol, growth rates of crime in a wide area network the Internet, are the fastest on the planet.

On average 80% of successful computer invasions into federal computer systems happen because of errors in the software or its poor quality.

According to most of experts cyberterrorism – turns into serious threat for mankind, comparable with nuclear, bacteriological and chemical weapon, and extent of this threat owing to the novelty, not up to the end is still realized and studied. We will consider the most frequent threats of the Internet and measures of counteraction.

Important element of system of measures of fight against computer crime are measures of preventive character, or a prevention measure. Most of foreign experts indicate that it is much easier and simpler to prevent computer crime, than to open and investigate it.

Usually allocate three main groups of measures of prevention of computer crimes: legal; organizational and technical and criminalistic, making in total the complete system of fight against this socially dangerous phenomenon(Nomokonov, 2003: p.104-110).

Now there is an active work on improvement not only legislations on fight against computer crimes, but also development of programs which can automatically reveal criminal encroachments. The government of the State of New Jersey (USA) which has already allocated 2,6 mln. dollars of the USA for the embodiment of the project in life became the sponsor of the new project on fight against hackers.

Experts call five main directions of legal regulation of the Internet relations(Lopatina, 2006: p.20) : protection of personal data and private life in Network; regulation of electronic commerce and other transactions and ensuring their safety; protection of intellectual property; fight against illegal contents of information and illegal behavior in Network; legal regulation of electronic messages.

The strategy of the international cooperation in the sphere of counteraction of computer crime and the priority directions her realization, including: interstate agreements, the organization of interstate operational search activity, adoption of interstate regulations and improvement of integration processes within the interstate organizations, justification of need of development and adoption of the appropriate comprehensive interstate program.

Thus, it is possible to draw a conclusion that fight against computer crime is connected as with use of the traditional means applied by the states (within the existing international organizations and also on the basis of bilateral contracts on legal aid and multilateral contracts concerning fight against separate types of offenses and to rendering legal aid on criminal cases), and with creation of new, more effective remedies of counteraction to this type of crimes.

References

1 Security Gazette, 1980. September. – P. 7.

2 Computer Law and Security, 1991. June. – PP. 2-3.

3 Selivanov N. Problems of fight against computer crime // Legality, 1993. – No. 8. – P. 36.

4 Vekhov B.V. (1996) Computer crimes: ways of commission, investigation technique. – M. – P. 44.

5 Baturin Yu.M. (1991) The right and policy in a computer circle. – M. – P. 134.

6 Lapshin S.I. Crime in the field of information technologies // Technologies and means of communication, 1997. – No. 1. – P. 107.

7 Starostina E.V., Frolov D. B. (2005) Protection against computer crimes and cyberterrorism. – M.: Eksmo publishing house. – P. 89.

8 Sabadash V. Computer crime: threats and forecasts//www.crime-research.ru

9 Lopatina T. M. Criminological and criminal and legal bases of counteraction of computer crime. The abstract on competition ю. M. N: 2006. – P. 16.

10 Dulov A.V. (1973) Bases of the psychological analysis on preliminary investigation. – M.: Yurid. litas. – 168 p.

11 Methodical recommendations for law enforcement officers of the State Parties of the CIS about the analysis and forecasting of a criminogenic situation and introduction in this activity of modern scientific methods//Research Centers of the All-Russian Research Institute of the Ministry of Internal Affairs of the Russian Federation. – 2012. – No. 1. – Page 2, 3.

12 Goben F. Op. cit. – P. 57-72; Scbwartau W. Information Warfare: Chaos on the Electronic Superhighway. – NY, 1994. – P. 215-248.

13 Osipenko A.L. Fight against crime in global computer networks: International experience: Monograph. – M.: Norm, 2004. – P. 152.

14 Nomokonov V. A. (2003) Current problems of fight against cyber crime//Collection of scientific works of the international conference «Information Technologies and Safety». Release 3. – Kiev: National Academy of Sciences of Ukraine. – P. 104-110.

15 Lopatina T. M. (2006) Criminological and criminal and legal bases of counteraction of computer crime. The abstract on competition. M. N. – P. 20.