ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com
Journal DOI: 10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

DETERMINANTS OF CRIMES IN THE SPHERE OF INFORMATION TECHNOLOGIES AND SAFETY.

Rasulev Abdulaziz Karimovich.
Candidate of jurisprudence, independent applicant of "Criminal Law and Criminology" department of the Tashkent State University of Law.

Manuscript Info

Manuscript History:

Received: 15 February 2016
Final Accepted: 29 March 2016
Published Online: April 2016

Key words:

Corresponding Author

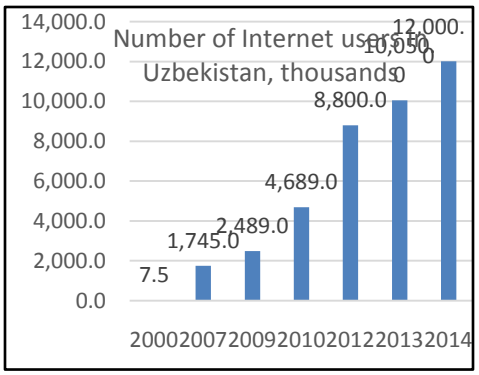
Rasulev Abdulaziz Karimovich.

Abstract

Introduction:-

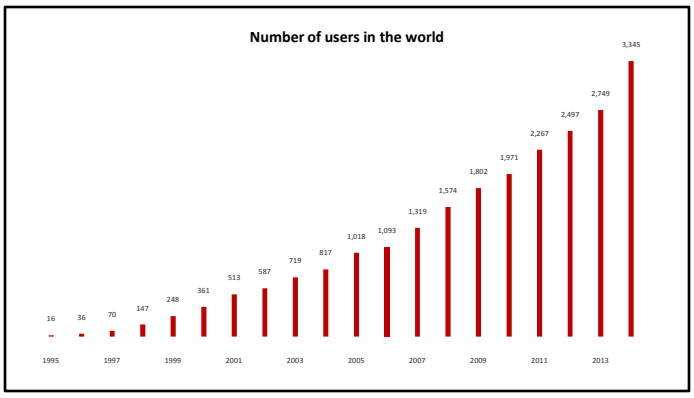
Despite the increasing, changing and modernizing of crime in the real world year by year, the virtual world doesn't lag behind too. And though Uzbekistan was not the first country in attempt to subdue virtual spaces, our experts in this area, hackers, don't concede in anything to their western colleagues, and even surpass them in some cases.

In the Republic of Uzbekistan development of information technologies goes at fast speed. As the head of state I.A. Karimov notes "Special attention has to be paid on implementation of the Comprehensive program of development of National information and communication system of the Republic of Uzbekistan for 2013-2020. It is necessary to continue works on further increase in technical capabilities of access to the Internet, expansion of optical networks of broadband access and construction of fiber-optical communication lines, to finish the translation of all regions, including remote areas, to digital television".[1]



[1] The report of the President of the Republic of Uzbekistan Islam Karimov at the meeting of the Cabinet of Ministers devoted to results of social and economic development of the country in 2014 and to the priority directions of the economic program for 2015. "Our priority task is creation in 2015 of wide opportunities for development of private property and private business by implementation of radical structural restructurings in national economy, consecutive continuation of processes of modernization and diversification".

Results of the undertaken measures on the development of information and communication sphere also should be noted in particular. According to the data of the Ministry of development of information technologies and communications, the number of Internet users in Uzbekistan has exceeded 12 million while the number of subscribers of mobile communication in the country makes more than 22 million, and the quantity of the households having the computer makes 37,4%, Internet access now — 58,1%.[2]



If to consider the figures on a global scale, then according to the Internet world stats website there are 3,345,832,772 Internet users in the world that makes 46.1% of the population of Earth (the population of Earth - 7,259,902,243 people) out of them, 2 billion live in developing countries.[3] China is holding the first place in the world in Internet audience number for five years. As of June, 2015, the number of Internet users in China has come up to 668 million people (population of the People's Republic of China - 1 285 million people). In a Top - 10 countries on number of Internet users: China - 668 million, India - 350 million, the USA - 277 million, Japan - 110 million, Brazil - 110 million, Russia - 87,5 million, Germany - 72 million, Indonesia - 71 million, Nigeria - 70 million, Mexico - 59 million (concerning China according to Information center of the Internet of China). [4]

Such mass character of use of personal computers, laptops and other computer equipment of personal appointment, not only in our country, but also in the whole world, leads to the parallel growth of cybercrime.

The problem of crime reasons is one of central in criminology. The causal complex of crime includes its reasons and conditions which in total make crime factors. The reasons are social and psychological determinants which directly generate, reproduce crime as the natural consequence; conditions are such social phenomena which don't generate crime and crimes, and promote, facilitate, intensify formation and action of the reason.[5]

According to a number of scientists, the most typical reasons and conditions of committing a crime in the sphere of computer information are:
• growth of number of the ICT and as a result increase in volumes of information processed and kept in ICT;
• insufficiency of measures for protection of ICT, ICT systems and their networks;
• insufficiency of protection of the software;
• growth of information exchange through world information networks;
• derogation from the technological modes of information processing;
• absence, imperfection or derogation from service regulations of programs for ICT, databases and hardware of ensuring network technologies;
• absence or discrepancy of means of information protection of her category;
• violation of the rules of work with the computer information protected by the law;
• low level of special training of officials of law enforcement agencies who have to warn, open and investigate crimes in the sphere of computer information;

[2] http://www.gazeta.uz/2015/09/18/users/
[3] http://www.itu.int/net/pressoffice/press_releases/2015/pdf/17-ru.pdf
[4] http://www.internetworldstats.com/stats.htm
[5]Криминология : учебник / под ред. Н. Ф. Кузнецовой, В. В. Лунеева. 2-е изд., перераб. и доп. М. :ВолтерсКлувер, 2005. С. 167–168.

• lack of a state policy in the sphere of ensuring information security.
Along with the above-mentioned, experts allocate the following reasons promoting commission of crimes of this look, it:
• insufficient protection of means of e-mail;
• negligence in work of users of ICT;
• unreasoned personnel policy in issues of employment and dismissal;
• violation of a production cycle of design, development, tests and delivery in commercial operation of computer systems;
• combination of functions of development and operation of the software within one structural division;
• violation of terms of change of passwords of users;
• violation of established periods of storage of copies of programs and computer information, and sometimes their total absence;
• groundlessness of use of ICT in concrete technological processes and operations;
• lack of due control from administration of activity of the workers involved at sensitive stages of processing of computer information;
• psychologically wrong interpersonal relationship of officials with subordinates and other workers. [6]

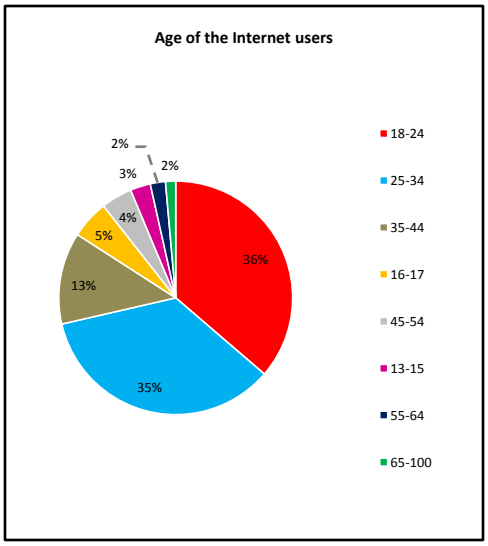
In this work, we will review two main reasons for cybercrimes. One of them, as it was already told above, growth of number of users. In sociology there is "a Rule of 15%", according to it if the population of Earth grows up for 15%, then the number of the committed crimes will grow up for 15%. This rule is also applicable also for cybercrimes. For 2014 the number of hacker attacks has reached 117330 attacks a day. It is stated in the report prepared on the basis of poll of 9800 IT services of the companies in 150 countries. In comparison with 2013 this number has grown twice. [7]

According to the estimates of world expert analytical centers, every second 18 users senior than 18 years become the victims of cybercrime, thus, daily more than 1,5 million people suffer from actions of cybercriminals. The number of the victims for 2014 makes about 378 000 000 people, each of whom lost $ 298 on average. [8]

According to the annual report of the Symantec company, the number of cyberattacks and cybercrimes against large companies in 2014 has grown around the world by 40%. Around the world experts have assessed the general damages of users from cybercrimes 400 billion dollars. This sum makes about 15-20% of the general contribution of the Internet to world economy which is estimated at 2-3 trillion dollars a year (0,5% of world GDP). According to CSIS, the damage share from cybercrime approaches already indicators of drug traffic and distribution of a counterfeit[9]:

№	Kind of Activity	Damage, % of GDP
1	International crime	1,2
2	Drugs	0,9
3	Fake/piracy	0,89
4	Cybercrime	0,8
5	Sea piracy	0,02

[6] «Причины и условия совершения преступлений в сфере компьютерной информации» А.В. СИЗОВ, Информационное право #2(13), http://cbb.vuit.ru/inform/?p=02002
[7] http://www.rg.ru/2014/11/12/hakeri-site-anons.html
[8] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
[9] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf



According to expert analytical centers, education level of the people who have committed computer crimes is characterized by the following data: lower than 7 classes – 3%, from 7 to 8 classes – 6%, 10 classes – 9%, an average special – 17%, incomplete the highest – 1%, the highest – 64%.[10] Now crimes in the sphere of use of computer technologies are committed five times more often than most of those having higher technical education (53,7%), or incomplete higher education (19,2%). However, the share of women in their quantity increases recently. It is connected with vocational guidance of some specialties and positions equipped with the automated computer workplaces which to a bowl borrow women (the secretary, the accountant, the economist, the manager, the cashier, the controller etc.). [11]

In our opinion, the question of age of the committers of computer crimes deserves attention. It is known that for all crimes in the sphere of computer information criminal liability is established from 16 years. At the same time, dependence of growth of number of socially dangerous acts on increase in the number of ICT park and growth of total number of ICT users, the ICT systems or their network allows to suggest the legislator to reduce the age of criminal liability. The curve characterizing age distribution of network criminals demonstrates that 20% are the users at the age of 14 - 18; 57% - for 19 - 25 year olds; 15% - for 26 - 35 year olds and 8% - for 36 - 55 year olds[12]. Studying of the subject "Informatics" within the school program from early school age allows to claim that the teenager has an opportunity to realize public danger of the actions in this sphere. In our opinion, if not for all computer crimes, then, at least, for creation, use and distribution of malicious applications people have to be subject to criminal responsibility if they have reached the age of 14 years by the time of commission of crime.

If to analyze crimes committed by young people aged from 14 till 25 years, most of them are on the Internet– 77%[13]. At this age, people feel especially high need for self-affirmation, aspiration to receive the maximum quantity of the vital benefits at absence, or incomplete character of some moral or legal constraining beginnings. It is quite adequate with today's information threats and infringement of information security of the country. Johnathan Joseph James who has begun to crack information systems from the earliest age can be a striking example. He cracked serious organizations, including Agency on reduction of military threat which is one of the divisions of the Ministry of Defense of the USA. After that, he obtained access to the names and passwords of users, and an opportunity to look through confidential information. On June 29 and 30, 1999 James attacked NASA, at that time he was 15 years old. He managed to get access, having cracked the password of the server belonging to the government agency located in the State of Alabama. James could wander freely about a network and steal several files, including a source code of the international space station.

[10]Северин В.А. Правовое обеспечение информационной безопасности предприятия: Учебно-практическое пособие. М.: Городец, 2000 – С.126.

[11] Министерство Внутренних Дел Республики Узбекистан Академия Р.К. Кабулов, Э.С. Абдурахманов «Преступления в сфере информационных технологий» Ташкент 2009 г.

[12] Ястребов Д.А. Неправомерный доступ к компьютерной информации: уголовно-правовые и криминологические аспекты: диссертация кандидата юр наук М.: 2005.

[13] Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. – М.: Норма, 2004 -С.163-164.

According to the statement of NASA, the cost of the software stolen by James is estimated at 1,7 million dollars. After detection of breaking of NASA it was necessary to disconnect system for check and restoring its working condition that has cost $41000. James was caught quickly as NASA made everything that to stop him. Johnathan became widely known for he became the first minor sent to prison for "hacking" in the USA at the age of 16[14].

Proceeding from it, the circle of people, committing crimes in the sphere of information technologies, is rather wide. As appears from the above-stated data on age and the identity of the subject of a crime, the considered group of crimes is committed by representatives of various sectors of society, and the age of offenders fluctuates from 14 to 55 years, and their level of preparation — from the beginner to the professional. A potential criminal in the field of the computer equipment is the person of any age having at least the minimum knowledge in this area. At the first international conference of the Interpol on computer crime, computer criminals have been conditionally divided into three age groups:

1) the youth aged from 11 till 15 years is generally commit thefts through credit cards and telephone numbers, cracking codes and passwords mostly out of curiosity and self-affirmation

2) people aged from 17 till 25 years. Generally, they are students who, for increasing of the informative level, come into close contacts with hackers of other countries on the Internet.

3) people at the age of 30-45 years which deliberately commit computer crimes for the purpose of obtaining material benefit, and also for the sake of destruction or damage of computer networks. [15]

But except users, it is possible to refer to an insufficient regulation rate of norms of the international and national criminal law as the reason. Today, some international legal bases of cooperation in fight against computer crime are fixed. In particular, the Convention of the Council of Europe on cybercrime of 2001[16], Measures for fight against the crimes connected with use of computers, accepted by the United Nations on the Eleventh Congress for the prevention of crime and the treatment of offenders in Bangkok on April 25, 2005[17], the Global program of cybersafety approved by the International union of telecommunication in 2007[18], the Okinawa Charter of global information society accepted on July 23, 2000 on Okinawa (Japan) [19], etc. On the scale of the CIS countries the Model criminal code was adopted on February 17, 1996 at the VII plenary session of Inter-parliamentary Assembly in which responsibility for computer crimes is regulated[20]; On June 1, 2001 in Minsk the Cooperation agreement of the State Parties of the CIS in fight against crimes in the sphere of computer information has been concluded[21]. In the Convention of the UN against a transnational organized crime of 2000, cybercrime problems made by organized criminal groups are indirectly considered by the adopted Resolution 55/25 of General Assembly of November 15, 2000.[22] Seeing these, we can draw a conclusion that there is no uniform international act which could unify norms on fight against cybercrime today.

Besides, in many states of the world there are laws authorizing illegal activity in virtual space. Laws of Florida and Arizona, states of the USA, "Computer crime act of 1978" establishing criminal liability for crimes in the sphere of

[14] https://ru.wikipedia.org/wiki/Джонатан_Джозеф_Джеймс

[15] Гаврилин Ю.В. Преступления в сфере компьютерной информации. Квалификация и доказывание. – М.: Книжный мир, 2003– С.88.

[16] Конвенция Организации Объединенных Наций против транснациональной организованной преступности от 15 ноября 2000 г. // Международное право и борьба с преступностью: Сб-к документов/Составители: А.В. Змеевский, Ю.М. Колосов, Н.В. Прокофьев. – М.: Международные отношения, 2004. – 720 с.

[17] Винник В. Виртуальные преступления // Юстиция Беларуси. - 2001. - № 4. – С. 13

[18] Из Балтимора депортируют русских киберпреступников // Webplanet.ru от 01.10.2007

[19] Старостина Е.В., Фролов Д.Б. Защита от компьютерных преступлений и кибертерроризма. – М.: Изд-во Эксмо, 2005. – 192 с.

[20] Конвенции СНГ «О правовой помощи и правовых отношениях по уголовным, гражданским и семейным делам» от 7 октября 2002 г. // Содружество. Информационный вестник Совета глав государств и Совета глав правительств СНГ. - № 2(41). - 2002 г. – С. 3

[21] Ямбулатова Н. В МВД Азербайджана создано управление по борьбе с киберпреступностью // http://www.crime-research.ru от 08.01.2008

[22] The European Convention on Cybercrime // http://conventions.coe.int/Treaty/EN/Treaties-/Html/185.htm

computer information, "The law on fraud and abuse with use of computers", the main legislative act establishing criminal liability for crimes in the sphere of computer information. Subsequently, it became the main regulatory legal act establishing criminal liability for crimes in the sphere of computer information, included as § 1030 in the Title 18 of the Code of laws of the USA[23], "The act of protection of national information infrastructure", and "The act of the patriot" 2001. (Patriot Act of 2001)[24] which, in addition, includes a special Chapter "Computer crime and intellectual property".

"The act of computer abuses" has been working in Great Britain since August, 1990. The first paragraph of this Act concerns "unauthorized access to computer data".

Liability for these crimes is provided by Chapter XX^1 the Criminal Code of the Republic of Uzbekistan, which is called "Crimes in the sphere of information technologies". Criminal sanctions at the national level do not provide reliable protection against computer crime yet because in the existing rules of law there is no enough articles about computer crimes, accurate classification of computer crimes, and complexity of interpretation and application of the existing articles is limited by actions of law enforcement agencies. The legislature has to carry out systematic work not only on development of new precepts of law, but also on the corresponding sanctions and simultaneous creation necessary mechanism of ensuring activity of law enforcement agencies, prosecutor's offices, judicial and retaliatory authorities which could pursue and punish effectively people guilty of committing crimes in the sphere of information technologies.

Criminal laws have to be supplemented with the corresponding civil sanctions. Absence of special instructions on an electronic form of transactions in the existing Civil Code of the Republic of Uzbekistan creates additional difficulties of recognition evidentiary force behind them. Adoption of the laws "On Electronic Commerce", "On Digital Signature", "On Electronic Document Flow", "On Appeals of people and Legal Entities", "Law on the Electronic Government" hasn't corrected the situation fully yet, since it is still necessary to change a number of articles of the code. Moreover, under the provision of some articles, the lawful part of fault can formally be imputed also to the victim as the legal entity who hasn't taken reasonable measures of precaution and also owing to the fact that the ICT and other equipment admits a source of the increased danger, users, being guided by imperfection of the law, seek to help, in return, not so much to representatives of justice how many to adhere to a neutral position. Besides, in all above laws it is said that the people guilty of a violation of the law bear responsibility in accordance with the established procedure. Unfortunately, the Criminal Code along with the Code on Administrative Responsibility do not have such norms.

Taking into account the above mentioned, and in the view of special relevance of the sphere of information technologies, to safety dynamically accruing informatizations of society and developing in this regard new forms and methods of computer crimes set scientific and practical and academic circles thinking, to combine seriously efforts on the international cooperation, interaction of the appropriate specialized authorities which are carrying out fight in this sphere.

One of conditions of creation of effective system of the international information security is development and adoption of the modern, universal international legal act providing adequate protection against new threats, but considering national sovereignty of the states in difference from the outdated European convention on cybercrime. The conclusion of the universal international treaty on fight against computer crimes which would consider already saved up experience of the international agreements in the field and features of the national legislation of member countries, quite complex and labor-consuming challenge. The separate Convention of the UN on counteraction to computer crimes which at the international level would help to fight in a complex and systemically could become such universal regulator and to counteract cybercrime and cyberterrorism.

For the analysis of cybercrime, exchange of information about it between the participating countries of the CIS, the analysis of the preventive measures and expeditious actions taken at the national level, and also carrying out special

[23]Номоконов В.А. Глобализация информационных процессов и преступность. – Киев: Информационные технологи и Безопасность, 2002. - С. 98

[24]Computer Crime and Intellectual Property Section. Комментарии к новым правилам, установленным Патриотическим Актом (США) 2001 г., в сфере компьютерной преступности и электронных доказательств // www.crime.vl.ru----

training of law enforcement officers, judicial and public prosecutor's shots it is necessary to create the Regional coordination center for counteraction of cybercrime within the CIS.

Creation of this Center will allow to carry out systemically collecting, data processing, rendering information, technical and criminalistic support of law enforcement agencies of the CIS countries to the relevant divisions, coordination of joint investigations, and also specialized training and training of specialists. The center can promote carrying out necessary researches and creation of the software, to be engaged in an assessment and the analysis of the existing and potential threats, drawing up forecasts and release of preliminary preventions. The field of activity of the Center will also include the help to judges, prosecutors and law enforcement officers.

Thus, the international cooperation in the sphere of fight against computer crime and in the sphere of ICT has to go on the way of expansion of forms of legal aid between the states, by means of the conclusion of new agreements or modification in already existing, and also creations of joint institutes on interaction in the sphere of fight against computer crime and to settlement of the disagreements arising in the course of application of such agreements.

Bibliography:

1. Criminology: the textbook / under the editorship of N. F. Kuz-netsovy, V. V. Luneeva. 2nd prod., reslave. and additional M.: Volterskluver, 2005. Page 167-168.
2. "The reasons and conditions of commission of crimes in the sphere of computer information" A.V. Sizov, the Information right #2 (13), http://cbb.vuit.ru/inform/?p=02002
3. Severin V.A. Legal support of information security of the enterprise: Educational and practical grant. M.: Gorodets, 2000 – Page 126.
4. Ministry of Internal Affairs of the Republic of Uzbekistan Academy R. K. Kabulov, E.S. Abdurakhmanov of "Crime in the sphere of information technologies" Tashkent 2009.
5. Hawks D. A. Illegal access to computer information: criminal and legal and criminological aspects: thesis of the candidate юр M.'s sciences: 2005.
6. Osipenko A.L. Fight against crime in global computer networks. – M.: Norm, 2004 - Page 163-164.
7. Gavrilin Yu.V. Crimes in the sphere of computer information. Qualification and proof. – M.: Book world, 2003 Pages 88.
8. The United Nations Convention Against Transnational Organized Crime of November 15, 2000//International law and fight against crime: Sb-k documents/originators: A.V. Zmeevsky, Yu.M. Kolosov, N. V. Prokofiev. – M.: International relations, 2004. – 720 pages.
9. Conventions of the CIS "About legal aid and legal relations on criminal, civil and family cases" of October 7, 2002//the Commonwealth. Information bulletin of Council of heads of states and Council of CIS Heads of Government. - No. 2(41). - 2002 – Page 3
10. Vinnik V. Virtual crimes//Justice of Belarus. - 2001. - No. 4. – Page 13
11. Starostina E.V., Frolov D.B. Protection against computer crimes and cyberterrorism. – M.: Publishing house "Exmo", 2006 – 192 pages
12. Yambulatova N. V. Ministry of Internal Affairs of Azerbaijan management on fight against cybercrime//by http://www.crime-research.ru from 1/8/2008 is created
13. Nomokonov V.A. Globalization of information processes and crime. – Kiev: Information technologists and Safety, 2002. - Page 98
14. See: Computer Crime and Intellectual Property Section. Comments to the new rules established by the Patriotic Act (USA) of 2001 in the sphere of computer crime and electronic proofs//www.crime.vl.ru
15. From Baltimore deport the Russian cybercriminals//Webplanet.ru from 10/1/2007
16. The European Convention on Cybercrime//http://conventions.coe.int/Treaty/EN/Treaties-/Html/185.htm
17. http://www.gazeta.uz/2015/09/18/users/
18. http://www.itu.int/net/pressoffice/press_releases/2015/pdf/17-ru.pdf
19. http://www.internetworldstats.com/stats.htm
20. http://www.rg.ru/2014/11/12/hakeri-site-anons.html
21. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
22. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
23. https://ru.wikipedia.org/wiki/Dzhonatan_dzhozef_dzheyms