www.tadqiqot.uz
ISSN: 2181-9130
2017№8

THE PERSONALITY OF THE CRIMINAL COMMITTING COMPUTER CRIMES

Rasulev Abdulaziz Karimovich

Independent researcher of Tashkent state university of law

ARTICLE DOI http://dx.doi.org/10.26739/2181-9130-2017-8-8-9

Annotation: The present article analyses essence and distinctive features of the personality of the criminals who committed computer crimes. Character trait of the personality, social features, technical expertise, motivating factors were considered as important factors. In the conclusion, the author proves importance of studying of the identity of the criminal for prevention of crimes in the specified sphere.

Key words: information technologies, information safety, computer, personality, Internet.

КОМПЬЮТЕР ЖИНОЯТЛАРИНИ СОДИР ЭТГАН ЖИНОЯТЧИНИНГ ШАХСИ

Расулев Абдулазиз Каримович
Тошкент давлат юридик университети мустақил изланувчиси

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

Аннотация: Мазкур мақолада компьютер жиноятларини содир этган жиноятчилар шахсининг моҳияти ва фарқли жиҳатлари таҳлил этилган. Муҳим омиллар сифатида шахс жиҳатлари, ижтимоий ўзига хосликлар, техник ноу-хау, рағбатлантирувчи омиллар кўриб чиқилган. Хулосада муаллиф кўрсатилган соҳадаги жиноятларни олдини олишда жиноятчи шахсини ўрганиш аҳамиятини асослантирган.

Калит сўзлар: ахборот технологиялари, ахборот хавфсизлиги, компьютер, шахс, Интернет.

ЛИЧНОСТЬ ПРЕСТУПНИКА, СОВЕРШИВШЕГО КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

Расулев Абдулазиз Каримович
самостоятельный соискатель Ташкентского государственного юридического университета

Аннотация: В настоящей статьи были проанализированы сущность и отличительные особенности личности преступников, совершившим компьютерные преступления. В качестве важных факторов были рассмотрены черты личности, социальные особенности, техническое ноу-хау, мотивирующие факторы. В заключении автор обосновывает важность изучения личности преступника для предупреждения преступлений в указанной сфере.

Ключевые слова: информационные технологии, информационная безопасность, компьютер, личность, Интернет.

Crimes in the sphere of information technologies and safety are characterized by the high level of latency.

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

Therefore, the official statistics does not give the chance to obtain the relevant data on criminological feature of persons who commit crimes in sphere of information technologies. It happens because of lack of appropriate statistics and high latency of such crimes.

A.N.Kosenkov and G.A.Cherny specify that in the conditions of a cyberspace the psychological content of interrelations the criminal — a crime subject and the criminal – the victim which of straight lines turn into mediated significantly changes: the criminal – the electronic device (Network) – the victim that leads to elimination of a material component both actions of the person, and social interaction. At the same time, «virtual» objects psychologically seem more available, including for illegal taking by them[1].

According to the traditional criminological theory, personal qualities and the external environment gradually define motivation of the decision to commit a crime in sphere of computer technologies. The motivation includes process of origin and formation of an occasion of criminal behaviour and its aims[2].

The profile of the cybercriminal represents is the description of features of the criminal committing crimes in the sphere of information technologies and safety. It is psychological assessment of certain features, which in total characterize the identity of cybercriminals. At the criminological characteristic of criminals in the sphere of information technologies and safety, it is necessary to proceed from the following four factors exerting impact on formation of the offender in information and communication space:

[1] Kosenkov A.N., Cherny G.A. General characteristic of psychology of the cybercriminal. Criminological magazine OGUEP, 3 (21), 2012 – P. 88
[2] http://digitalcommons.law.uga.edu/stu_llm/59/

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

Character trait of the personality: character trait, congenital at the person and psychological features of the person, which combined, contribute the personality for commission of illegal acts. Character trait of criminals in the sphere of information technologies and safety allow us to distinguish the following types:

1. «Beginner». This category of the personality commits offenses for the first time and characterized by use of various computer technologies for the personal consumer purposes – for loading of music, games or applications. Generally these teenagers or youth at the age of 15-25 years. Sex – in most cases men's. Education – an average, average special or the highest.

2. «Fan». This category of the personality represents people who periodically commit offenses in computer network, generally is technicians (system administrators, technical consultants). Males (more rare than women's) aged from 20-30 years enter into this group. Formation of «fans» comes from skills of the past as «beginner» or in connection with vital circumstances (performance of instructions and «orders»).

3. «Professional» – category of the professional persons, on a professional basis who are engaged in illegal activity and called hackers. It is a class of the educated persons knowing all elements of computer programming and technical work. Age – 25-40 years. Sex – in most cases men's. Ayala Karissa fairly notes that high technical readiness – their main line, high latency of crimes – a basis of their motivation, internal predisposition – the main condition of the introduction on the criminal way, and a social and economic situation in the country – the main reason for the final choice[3].

[3] Ayala, Karissa, «Cybercrime» (2004). LLM Theses and Essays. 59.

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

Proceeding from the above-stated three groups, it is possible to define that the cybercriminal is characterized by technical readiness, possesses a set of the methods allowing it to carry out various frauds (receiving unauthorized access, breaking of security keys, etc.). In most cases, it is the graduate (or the student of older years) technical college having the personal computer or the laptop. In most cases are men at the age of 15-40 years.

Age of the persons who committed crimes in the sphere of information technologies and safety is important. For definition to the age characteristic, we will address statistical data concerning Internet users.

Now more than 3,488 billion people around the world have an Internet access that is the average global level of penetration is 35 per cent. According to sources, North America and Western Europe are global areas with the highest Internet indicators of use of a segment of worldwide network – about 80 per cent, whereas in the Southern Asia the indicator of this level is low[4].

According to analytical these 26,5% of Internet users in the world make faces aged from 10 up to 24 years, 26,7% of users – from 25 to 34 years, 20,4% - from 35 to 44 years[5]. As we see a large number of Internet users make youth. Definition of the age characteristic of Internet users allows defining also potential subjects of crimes in the sphere of information technologies and safety.

In the Republic of Uzbekistan, the age of the subject of a criminal responsibility fluctuates from 13 to 18 years, at the same time the general age is 16 years. In England, it is possible to bring to trial from 8 years, in Greece – from 13 years, in Sweden – from 15 years, in Finland – from 16

[4] http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/
[5] http://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

years, in Egypt, Lebanon and Iraq, the USA – from 7 years, in Israel – from 9 years, in Iran, Turkey – from 11 years.

It should be noted that in world practice the tendency of decrease in age of the subject of crimes in the sphere of information technologies and safety is observed. It is promoted, in our opinion, by two reasons:

1) The Internet became an important and significant resource in youth life;

2) Recently the attacks from young hackers began to extend – school students and teenagers.

For example, in Belarus the age of criminal prosecution for plunder by use of the computer equipment and evasion from serving sentence in the form of restriction of freedom is reduced up to 14 years. According to the National centre of legal information, it is caused by growth of number of such crimes committed by minors[6].

According to some information in the USA, the group of young hackers (school students) which calls itself CWA cracked personal e-mail of the director of CIA John Brennan and the minister of a homeland security Jay Johnson[7].

Experts of one of the largest Russian media about IT and IT safety «HACKER» claim that most of hackers – just missing children who have too much free time. Only 10% of hackers give the report in the actions. 90% of acts of vandalism on the Internet are committed by 13 summer teenagers who need «to have a good time»[8].

Considering a question of the identity of the criminal and his signs, it is impossible to disregard opinion of the famous American specialist in fight against a phishing (a kind of computer fraud) Lens James considering that in the 21st century the greatest distribution among computer

[6] http://www.interfax.by/news/belarus/1200077
[7] https://russian.rt.com/inotv/
[8] https://xakep.ru/2016/07/19/13108/

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

criminals was gained by skriptkidd (script kiddies)[9]. It refers their early age, nonprofessional hacker abilities, existence of free time, persistence on achievement of a goal, use of already ready codes developed by experts to their main features.

Taking into account the broad involvement of youth into information and communication space, commission of various offenses and crimes by teenagers and youth it is necessary to reduce age of a criminal liability for crimes in the sphere of information technologies and safety up to 14 years.

Technical know-how: the factor connected with degree of technical knowledge of the software and espionage devices which are used by the personality for cybercrime commission. In this context, first of all, it is necessary to consider «hackers».

In legal literature the question of the identity of the criminal who committed crimes in the sphere of information technologies and safety, in other words the computer criminal is considered, generally through a prism of the isolated group of persons, called «hackers». Traditionally hackers are considered as a high-class group of professionals which use the mental abilities for development of ways and methods of implementation of illegal infringement of information and communication resources and networks. Mainly these breakings cause damage to the system of protection and safety of information technologies. Therefore, often hackers are called computer hooligans.

Analysing legal literature makes possible to mark out the following signs of the identity of the hacker:

- Existence of the purposeful, thought-over preparation for crime;

[9] Lens James. Technology of computer crimes. 2008. – P. 42

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

- Originality of a way of crime execution;
- Use as tools of crime execution of modern information and communication technologies;
- Rejection of measures to crime concealment;
- Facts of unmotivated mischief[10].

Except hackers, as computer criminals in the criminological theory allocate:

- persons who have no sufficient skills in the field of computer engineering and technical programming at the same time they have only some skills on narrow-minded use with means of the computer equipment. As a rule, their actions are directed to destruction, blocking, modification, copying by nothing to the protected information (for example if the computer has no password of access or the password is known to a wide range of persons);
- Persons who have mental deviations. Carry the persons having various computer phobias to their number. This category of diseases is connected with violations in information regime of the person under the influence of the external or internal destabilizing factors both the congenital, and acquired property.

Social features: the factor connected with influence of a social environment in development of criminal behaviour in the personality. As a rule, the studied persons have the closed character, are depressive, inclined to personal experiences, and are sensitive. Their achievements in school were not brilliant, but fundamentals of informatics and mathematics they learn well. In the majority, they have incomplete family where the difficult psychological atmosphere reigns. The legal nihilism, high self-esteem are characteristic of them, it is frequent they,

[10] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In 11th Workshop on the Economics of Information Security (WEIS), Article 10, Berlin, Germany, Jun 2012. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

feeling the impunity and invulnerability, neglect requirements of the provisions of the law and consider quite normal to define independently morality and correctness of these or those precepts of law, proceeding from own criteria. They often show infantilism, irresponsibility, uncompromising stand, misunderstanding of possible consequences of the actions, quite often ignore public opinion and interests. In similar cases, «assessment of the situation is carried out not from positions of social requirements, and proceeding from personal experiences, offenses, problems and desires»[11].

The excessiveness of a self-assessment conducts to the fact that some hackers make the studied acts spontaneously, without serious preliminary preparation, leaving some kind of «messages» to heads of security services of a subject to encroachment, they can publish in the Internet lists of the of «the victorious attacks» with concrete indications of dates of the organizations victims, and sometimes and methods of «breaking». The tendency to disclosure of this sort of information is connected with not unreasonable beliefs that law enforcement officers, anyway, cannot effectively use this information for investigation.

Nevertheless, the studied group of criminals has also a number of positive qualities of character, which, however, are directed not to the best. These people very brightly and unconventionally think, have very good preparation in the field of information technologies, differs in high performance, are persistent and persistent in achievement of the goal (they for hours can study ways and solutions of «breakings»). They have resistant antisocial no installation, aggression, they and in thoughts

[11] P.H.Hartel and M. Junger. Teaching information security students to «think thief». Technical Report TR-CTIT-12-19, CTIT, University of Twente, Jul 2012. http://eprints.eemcs.utwente.nl/22066/.

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

cannot allow commission of any violent crimes. In case of anticipation of high probability of approach of adverse consequence in law, many of these persons can refuse crime execution. It is possible to note with confidence that fear of responsibility is closely connected with degree of activity of determination of actions of law enforcement agencies and also a necessary share rigidity of repressive norms.

The motivating factors: various factors which force them to become cybercriminals. Let's consider some motivating factors:

Self-interest: This factor belongs to almost any offender, any person who illegally get financial profit on crime. On the one hand, it can include any bank employee who uses the office powers (computer access) to transfer money from fund of the account of one person to the own bank account, on the other hand – any foreign person malefactor which cracks the database of the company to steal data or other significant data which he can sell to other persons, that is professional «hackers mercenaries» who get profit on commission of these illegal actions. The criminal of almost any profile can be motivated with money – youth and old generation, persons men's and female, in independence of all personal social and economic and other signs. Criminals in the sphere of information technologies and safety very much differ from traditional criminals – swindlers or professional murderers.

Emotions: the most «destructive» cybercriminals often act on emotions: anger, revenge, «love» or despair. This category includes the rejected fans or the former spouses (cyber prosecution, terrorist threats, post prosecution, unauthorized accesses) angered or the dismissed employees (deleting of websites of the company, the Dos-attack, theft or destruction of data of the company,

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

influence of confidential information on the company), unsatisfied clients, the conflicting neighbours, students, angry consumers, etc. The group also includes people who are in virtual communication in social network group.

Sexual motives: The considered factor is connected with psychophysiological features and includes some the strongest of cybercriminals: consecutive tyrants, sexual sadists (even serial killers) and paedophiles. Children's pornographic authors can fit into this category, at the same time, they can also just use sexual impulses (to excite interest in viewing of materials of pornographic contents) other people for receiving profit, and in this case, their motive belongs to the «monetary» category.

Political and religious views: It is closely connected with category «emotions» because today people become very emotional concerning the political and religious beliefs. We know well that religious extremists are ready to commit disgusting crimes under cover of religion. It is usually a motivation factor for cyberterrorists, but also and motivates many other people for commission of crimes.

Today's Islamic radicals are completely informed on the tendencies, styles and mechanisms used on the Internet so can successfully use any platforms for involvement of bigger audience and distribution of the ideology.

The propaganda machine of IS effectively showed the awareness and competence of use of the Internet for the campaign aimed at the audience close to the western culture. For example, by means of «memes», usually comic character, are copied and quickly memes and from IS extend among Internet users[12].

«Only for an entertainment» (hooliganism): This motivation concerns teenagers (or to young hackers) and others which can hack networks to get illegal access to the

[12] http://365info.kz/2016/05/kiber-tehnologii-igil-ot-igr-do-nevidimogo-interneta/

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

protected author's right to music, movies, to erase websites etc. - not from malicious intention or financial benefit, and simply, «because they are able to do it». They can make it to prove the skills to adults or themselves, to them can be just curious, or they can consider the actions as a game. Though they purposely do not do harm, their actions can entail expenses for the companies, cause a grief of people and cause other damage.

Cybercriminals can use computers and information and communication networks or with intention to use them as the instrument of crime execution, or is casual by preparation for crime execution. Many crimes could be committed by cybercriminals without using computers and information and communication networks. For example, terrorist threats could be made by phone or through Internet mail; thieves could steal money of the company from the safe.

Even those crimes, which seem unique for information century usually, have prototypes in the period of time when the Internet did not exist[13]. Unauthorized access to the computer technically differs, but not so differs in thinking, motives and intention from unauthorized access (penetration) to vehicles, home office or the room (i.e. theft), and deleting of the website of the company is very similar in many respects to destruction of a facade of buildings of the company[14].

Unfortunately, it is possible to note that computer networks played the same role, which they played for lawful users of computers for criminals: they made work easier and more convenient.

---

[13] Computer crime: A criminological overview. Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Vienna: Citeseer. Hickey, E. W. (2009)

[14] Wood, R. A., & Wood, N. L. Stalking the Stalker: A Profile of Offenders-. FBI Law Enforcement Bulletin. Volume 71. Issue 12 , (2002). pp. 1-12.

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

Some cybercriminals use the Internet to find the victims. It includes swindlers, serial killers and all others. In other cases criminals use information and communication networks to keep account connected with the number of their crimes (the list of drug dealers or quantity of the sold goods) or for communication with potential clients or their accomplices in commission of crimes.

From the point of view of criminological science, it is interesting to consider cybercriminal thinking. Not all cybercriminals absolutely definitely think equally. Thinking and understanding by the criminal of the actions depends on various factors. For example, the child at teenage age loads in the illegal way of a song or a game to the Internet, really without understanding that the action made by it is illegal. The «desperate» employee who participates in various financial frauds, illegally getting access to the data which are a secret of the company to sell to the competitor carries out the actions purposely and the purposes of a personal profit. Some sociopaths or hackers commit various cybercrimes (breaking of the websites, blocking of information on the Internet) because of hooligan motives.

Often computer crimes are committed by an organized group of persons. George Newman notes that about 62% of computer crimes are committed as a part of organized groups[15]. Many hackers create criminal groups and make different crimes in partnership. At commission of cybercrimes, certain conveniences to malefactors have organization:

– Firstly, joint crime execution increases its quality and reduces time criterion;

[15] G.R.Newman. Cybercrime. In M.D.Krohn, A.J.Lizotte, and G.Penly Hall, editors, Handbook on Crime and Deviance, pages 551-584. Springer, Nov 2009. http://dx.doi.org/10.1007/978-1-4419-0245-0_25.

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

– Secondly, in organized group work in connection with cast at commission of cyber-attacks effectively returns to normal;

– Thirdly, members of organized group will regularly exchange knowledge and abilities, increasing the «criminal» potential.

Especially it is necessary to emphasize that Criminal code of the Republic of Uzbekistan provided as the aggravating circumstances crime execution in partnership – a group of persons or organized group in five of six articles of chapter XX[1] – Crimes in the sphere of information technologies[16]. Only in article 278[1] of Criminal code of the Republic of Uzbekistan (violation of the informational support rules), this circumstance is not allocated as aggravating.

Crime in the sphere of information technologies and safety is such big problem that some law enforcement agencies of foreign countries should devote activity of all divisions only to fight against these crimes. Criminals of the considered category often use means of the computer equipment to transmit signals for other accomplices easily to operate electronic databases illegally to appropriate the money or other things having material value. Many criminals in the sphere of information technology and safety are highly organized and qualified, abducting only the limited sums from any source, they can continue the activity for many years or decades, without being afraid of the fact that they can be caught.

So, the criminological characteristic of the persons committing crimes in the sphere of information technologies and safety taking into account results of various statistical and empirical researches, can become the strong base in activities for prevention and control of

[16] Criminal code of the Republic of Uzbekistan (source: http//www.lex.uz/)

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

offenses in the sphere of information technologies and safety, are used when developing appropriate programs of prevention and fight against the considered crimes.

References:

Criminal code of the Republic of Uzbekistan (source: http//www.lex.uz/)

Ayala, Karissa, «Cybercrime» (2004). LLM Theses and Essays. 59.

Computer crime: A criminological overview. Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Vienna: Citeseer. Hickey, E. W. (2009)

G.R.Newman. Cybercrime. In M.D.Krohn, A.J.Lizotte, and G.Penly Hall, editors, Handbook on Crime and Deviance, pages 551-584. Springer, Nov 2009. http://dx.doi.org/10.1007/978-1-4419-0245-0_25.

Kosenkov A.N., Cherny G.A. General characteristic of psychology of the cybercriminal. Criminological magazine OGUEP, 3 (21), 2012 – 260 p.

Lens James. Technology of computer crimes. 2008. – P. 42

P.H.Hartel and M. Junger. Teaching information security students to «think thief». Technical Report TR-CTIT-12-19, CTIT, University of Twente, Jul 2012. http://eprints.eemcs.utwente.nl/22066/.

R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In 11th Workshop on the Economics of Information Security (WEIS), Article 10, Berlin, Germany, Jun 2012. http://weis2012.econinfosec.org/papers/Anderson_WEIS 2012.pdf.

www.tadqiqot.uz
ISSN: 2181-9130
2017№8

Wood, R. A., & Wood, N. L. Stalking the Stalker: A Profile of Offenders-. FBI Law Enforcement Bulletin. Volume 71. Issue 12 , (2002). pp. 1-12.

Web-sources:

http://365info.kz/2016/05/kiber-tehnologii-igil-ot-igr-do-nevidimogo-interneta/

http://digitalcommons.law.uga.edu/stu_llm/59/

http://www.interfax.by/news/belarus/1200077

http://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/

http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

https://russian.rt.com/inotv/

https://xakep.ru/2016/07/19/13108/