Approach issues to criminalistic classification of computer crimes

Lola Furkatovna Tatarinova[1], Ermek Zheenbekvna Sokurova[2], Danila Vladimirovich Tatarinov[3], Tolkyn Amzeyevna Shagdarova[4], Anel Rakhmetzhanovna Yensebayeva [5], Dinara Osmanova [6]

[1]"Turan" University. St.Street 16-18-18a, Almaty city, 050013, Republic of Kazakhstan
[2]Kazakh Humanities and Law University. Korgalzhym Avenue, 8, Astana city, 010000, Republic of Kazakhstan
[3]Kazakh National University named after al-Farabi. Al-Farabi Avenue, 71, Almaty city, 050038, Republic of Kazakhstan
[4]Kazakh Humanities and Law University. Korgalzhym Avenue, 8, Astana city, 010000, Republic of Kazakhstan
[5]Kazakh-Russian University. Kabanbay Batyra Str., 8, Astana city, 010000, Republic of Kazakhstan.
[6]Kazakh University of Economy, Finances and International Trade. Yesenberlin Str., 2a, apartment 54, Astana city, 010000, Republic of Kazakhstan

Abstract. Due to appearance and extension of computer crime range the ways and methods of their commitment are improved. Criminalistic approaches do not always correspond to the facts and it leads to degrease of crime detection rate. Thus there is a great necessity to develop a special criminalistic classification of computer cyber crimes which will contribute to the improvement of their investigation process. The issues of struggle against computer crimes are specified by their transboundary nature, therefore, forming and development of computer crime investigation methods shall start with "fixing" of the universal classification which is conceptually difficult.
[Tatarinova L.F., Sokurova E. Zh., Tatarinov D.V., Shagdarova T.A., Yensebayeva A. R., Osmanova D. **Approach issues to criminalistic classification of computer crimes.** *Life Sci J* 2014;11(12s):391-395] (ISSN:1097-8135). http://www.lifesciencesite.com. 84

Key words: cyber crimes, information, criminalistic classification, track, investigation, variety.

Introduction

The important task for the law enforcement bodies in the condition of swift development of IT technologies is a counteraction to the crimes committed with their application. The key problem of their exposure and investigation is their transnational and transboundary nature as well as the considerable difference in the state legislations where the crime was committed and where the consequences were.

Strengthening of cyber security and protection of important information infrastructures of the state plays an important role for security and welfare of each country. Encreasing the Internet security and protection of the Internet users became a main part of new service development as well as the government policy [1; 2; 3]

In this case the problem solving of the criminalistic classification [4] used in the theory of information protection and information security [5] plays an important.

The problem concerning the essence and the meaning of criminalistic classification of crimes in whole and computer related crimes in particular is far from its logical decision. It is stipulated by the existence of many diverse scientific points of view which can be divided into two full-fledged groups: the first group of specialists adhere to the opinion that criminalistic classification of crimes is an element of criminalistic characteristic but the second group believes that the analyzed classification is a basis for creating both criminalistic characteristic [6;7] and particular criminalistic methods of crime investigation [8].

The existed disagreements are to a large extent due to a great number of bases for the classification.

In spite of difference in views most researchers hold the opinion that the acceptance of the dominant position of the criminal basis in the creation of the criminalistic classification plays a significant role.

Principal part.

To disclose and resolve the problem of computer crime classification it is necessary to start from considering the classification as a multilevel system whose upper level is formed on the basis of the criminal notion "corpus delicti".

In addition to that this approach makes pay attention to developing and supporting the strategies of cyber security which it itself is a very important element in struggle against cybercrimes [9].

The problem appeared are connected with the classification of the acts relating to the illegal use of ID numbers in cellular systems as far as these ID numbers are sent without any protection and can be got by any person who has a special set of techniques.

The European Community tried to develop a definite classification which was described Convention "About Cybercrimes" adopted by the

Council of Europe in November, 2001 in Budapest [10].

Besides in leading industrialized countries the law enforcement bodies have developed their own classification of the main types of cybercrimes reflected in two lists: "Minimal list of offences" and "Optional list of offences" and was officially consolidated as "Guidance of INTERPOL on computer related crimes".

Therefore "Minimal list of offences" includes the following computer crimes: fraud, falsification of computer information, damage of computer data or programs, computer sabotage, unauthorized access, unauthorized interception of data, unauthorized use of licensed computer programs, and unauthorized reproduction of schemes.

Optional list' includes: change of computer data or programs, computer espionage, illegal use of computer, and illegal use of licensed computer program.

The most widespread classification of computer crimes is a codifier of the working group of INTERPOL taken as a base for the automated information-searching system created at the early nineties.

The named international codifiers and systems of classification have acquired a grave shortcoming expressed in entering letter "Z" which led to the chaotic mixing of criminal principals and technical peculiarities of automatic data processing (from criminalistic point of view), and without doubt it will bring to considerable problems while defining the particular goals and objectives of the computer crime investigation.

These problems solving is primary important as far as the development of the full-fledged computer crime classification will favour the development of both criminalistic characteristics and particular criminalistic methods of crime investigation.

This opinion is stipulated by the fact that the criminalistic cybercrime classification shall embody a complete and consistent structurally-information model that reflects fundamental important elements of the given type of crimes and their mutual relations of nesting and subordination from criminalistic point of view.

The basis of the criminalistic classification shall be the analysis of the criminal trespass subject, i.e. computer data, as a complex multilevel subject which includes three main levels of presentation: physical, logical and semantic [11] and from exposure of a set of simple operations at every level.

Physical level – the level of material information carriers where information is presented in the specific characteristics of the substances or the electromagnetic field.

Taking into account that in fact all applied modern computers are digital and have the binary number system, therefore, great volume of data can be in the form of chain or elementary information unit field ("O" and "1").

From criminal point of view at this level the computer data exist only in the form of facts, information (Dato-level). For instance, while coping a "hard" disk a criminal using special means can read or copy the flow of binary data from magnetic carrier but it will be still for him as a comprehensive whole.

Logic level – the level with more complex structure (from byte to file) on the basis of elementary components of the physical level. The present level includes two groups of consolidation rules – general and specific. General rules are dictated by the physical principles of the equipment and the technical peculiarities of the used means of information handling and cannot be changed fast and at will.

From criminal point of view the present level can be characterized as a level of program means (Program-level) which implements the procedure of information processing of *Data-level*.

Semantic level – the level of the notional information presentation. The present level includes substantial part of computer information performed as a unity of two previous types (Block-level = Program level + Data-level where "+" is a mark of unity).

From criminal point of view only at this level the computer information "assumes the commodity form", i.e. its useful "consumer properties' become apparent in this form.

From our point of view such a presentation of computer information allows to take into account not only main criminalistic problems but all peculiarities of criminal classification of deeds in the sphere considered. Thus the existence of the semantic level of presentation allows to limit (in criminal sense) computer crimes from other information crimes committed with help of computer or new information technologies (divulgence of a secret of adoption as the result of access to the registry office data, industrial espionage or a blow of national safety, and etc.).

From criminalistics point of view the performed presentation allows to understand the nature of the phenomena which take place while committing a computer crime, to comprehend types and methods of track appearance and relying on it to define the most preferential way of crime investigation. It is not possible to get reasonable information (ready for the person's perception), i.e.

the semantic level, without overcoming two lower levels of its presentation.

Thus in case of lack or impossibility to expose even one of the elements of the suspected activity connected with computer crime commitment at lower level its presentation makes us doubt seriously in commitment of the crime personally at higher level and it testifies to the presence of an accomplice or a forced abettor. Presentation of information in the form of three-level system allows to define an exhaustive list of actions at any of them, therefore, to present any deed described in the criminal legislation or in other information disciplines as a set of elementary actions of the appropriate level.

Thus at the physical level of information presentation it is technologically possible to carry out only three actions – reading, recording, and deleting.

Having committed any mentioned deed the user of the automated information system shall execute all actions considered in the criminal classification and the latter by turn include the successive operations.

In accordance with the general scheme of data processing the basis of any information action is the triad: reading *(Read),* modification *(Modification)* and record *(Write).* Taking account the existence of different levels of information presentation (Data, Program, and Block-levels) we form the set of simple operations: R_d, R_p, R_b, M_d, M_p, M_b, W_d, W_p, W_b. Having complemented it with "empty" operations "nothing to read" R_o, "nothing to modify" – M_o и "nothing to write" – W_o,we get a complete basis for the construction of the criminalistic classification of computer crimes.

Then any crime can be described in the following way R_x, M_x, W_x, where X – any from the defined levels of computer data presentation.

Taking account all foresaid facts the criminalistic classification of computer crimes will be as follows:

1. Deleting (destruction) of computer information *(R_o M_o W_x).*

2. Illegal abstraction of computer information or infringement of the sole right to its use *(R_x M_o W_o).*

2.1. Illegal abstraction of computer information as a totality of information, documents – infringement of the sole right of possession *(R_d M_o W_o).*

2.2. Illegal abstraction of computer information as an algorithm (by means of transformation) *(R_p M_o W_o).*

2.3. Illegal abstraction of computer information as goods *(R_b M_o W_o).*

3. Action or act of omission relating to the creation (generation) of computer information *(R_o M_x, W_x).*

3.1. Spreading of computer information by means of telecommunication channels of data computer nets bringing damage to the subscribers *(R_o M_d W_d).*

3.2. Development and spread of computer viruses and other malicious software for the computer system *(R_o M_p W_p).*

4. Illegal modification of computer information *(R_x M_x,W_x).*

4.1. Illegal modification of computer information as a totality of facts, information *(R_d M_d W_d).*

4.2. Illegal modification of computer information as an algorithm (R_p M_p W_p).

4.3. Illegal modification of computer information as goods in order to use its useful features *(R_b M_b W_b).*

Let us consider the content of every mentioned type of computer crimes in detail.

Deleting (destruction) of the computer information is the most clear type of crime from criminal point of view because it embodies the physical destruction of information. From criminalistic point of view it is the most difficult type of crime as far as it does not leave any traditional tracks. It is because the aim of the crime is deleting of information including its track. However, deleting computer information of one type and tracks of its existence the criminal creates the tracks of another type specified by the environment of the computer information existence at the lower (detailed) level. Based on the qualification feature of the present crime *(R_o M_o W_x)* the main aim of the investigation will be the detection of the fact of deleting information and the discovery of instruments (means) of impact on information.

Illegal abstraction of computer information as a totality of information, documents (infringement of the sole right of possession). It is a widespread class of simple criminal deeds which are not paid proper attention to.

From criminalistic point of view it is the simplest action which can be carried out without any long preparation, qualification and development of special device. In this case it is possible to use a standard tool bag of hardware and software of the automated system where this action takes place. Their results can be record on the machine-readable data carrier (magnetic or laser disk, magnetic tape, and etc.), paper or simply to stay in the memory of the person.

Illegal abstraction of computer information as an algorithm (by means of transformation) The

present type of crime is related to acquaintance with the used analysis of any assessment, decision-making behaviour in the expert system or any automated system of decision-making.

From criminalistic point of view it is rather a difficult action because it includes not only the access to the information as a set of facts but to the following stages connected with analysis of the structure of the used data, clarification of their semantic meaning, the succession of their use in order to get the required result. To implement this action it is necessary to have special means of software analysis (debug tools, disassemblers, interpreters and etc.), and highly-qualified executors (or even one of them).

The computer crimes of such a type along form a plot for industrial espionage.

Illegal abstraction of computer information as goods.

It is the most widespread type of criminal deeds during which the computer programs or the whole information system (the data pool of the electronic archive) are copied without permission of the owner.

From criminalistic point of view it is a more serious deed during which it is necessary to use a machine-readable medium because new program products occupies a lot of memory space. To obtain the goal while committing the present deed it occurs not to be enough to misappropriate the files of the program product because it cannot work properly if there is no any definite components of the general (the drivers of the peripheral device, a musical card availability, and etc.) or general-systemic program mathematical software (database management system, a spreadsheet, and etc.).

All three described crimes have the classification indicator $(R_x M_o W_{o)}$. It means that their general indicator is the unauthorized coping of computer information. One of the main tasks during the investigation of the present types of crimes, therefore, is the search and the registration of identical sets of data or programs in the automated system of the "victim" or the 'criminal'.

Spreading of computer information by means of telecommunication channels of data computer nets bringing damage to the subscribers. A rather widespread deed of such a type is spreading of "spasms" that is spreading of obtrusive numerous and unnecessary advertising or other messages by e-mail.

The deed of such a type is a "telephonic piracy". It occurs when criminals carry out illegal connection to the municipal or intercity telephone network. If to analyze carefully the essence of the present deed it is possible to clarify that the illegal connection to the telephone lines is in creation of the definite information (of the data unit) which corresponds to the information of the true subscriber and its record in the computer of the house telephone system that is it corresponds fully with the classification index $(R_o M_d W_d)$.

Development and spread of computer viruses. This type of deeds is very widespread nowadays and it may compete relating to the quantity of the registered cases only with illegal abstraction of computer information as goods. The essence of the present crime is to write a special computer program possessing the ability to copy itself many times and to execute other functions set by the author (to shed letters from the visual display into one heap, and etc.).

Illegal modification of computer information as a totality of facts. The present type of crimes was especially widespread in the automated bank systems as far as exactly in them the records in the fields of the databases show the definite sums of money or other information which have the definite money or other economic means.

Illegal modification of computer information as an algorithm (by means of handling). The present type of the criminal deeds can happened much rarely and is committed not only to get any software but to analyze it preliminarily.

The typical criminal characteristics of the described crime are firstly, the area of the activity (scientific-technical development) where somebody else's idea (algorithm) shall be implemented into must acquire great economic or another importance.

Secondly, the executors shall possess different special skills in the described field.

Thirdly, to commit the crime of such a type it is necessary to possess special technical supply and software.

Illegal modification of computer information as goods.

The present type of activity as well as illegal abstraction of information as goods is the most widespread crime (from our point of view, it is exactly a crime). Many software firm-producers trying to protect themselves from the computer piracy develop and use different methods of protection from coping and analysis of their products. However the economical conditions in which our economic exists and fundamental impossibility to create ideal means of information protection lead to the fact that having got software or database legally (or half-legally) once we modify it in such a way that it allows to be copied many times and to use useful properties of information as goods without any limitations (temporally or relating to the number of triggering) which were done formerly by the developer.

However in practice there are such crimes which were not included in the analyzed classification scheme. For example, it is distortion of information while conducting information wars, i.e. "cyber manoeuvre" [6].

For example, such a type of computer crime commitment as distribution of the harmful program "Trojan horse" and its acquisition by means of "screenshots" (i.e. getting images for display screens while the user is working) is a succession of two criminalistic important elements:

• creation (adjustment) of the harmful program (precisely the server part of "Trojan horse") and its distribution to addressees $(R_o\ M_p\ W_p)$;

• getting a message from the infected computer, adjustment and execution of the commands by means of the client's part of the "Trojan horse" $(R_d\ M_p W_d)$.

In this case the described criminal deed can be performed as follows: $(R_o\ M_p\ W_p - R_d\ M_p W_d)$.

Conclusion.

The use of the described way differs radically from the existed one for a variety of reasons.

Firstly, in the offered way of the criminalistic classification the specific character of the crime commitment environment defines properly the potential types of crime commitment and as the result it allows to specify smaller (elementary) actions but important from criminalistic point of view. In addition to that the characteristics of these elementary actions and their possible combinations form the unique criminalistic image of the computer crime.

Secondly, the offered way of the criminalistic classification allows to get the formalized definition for every of these elementary actions and it will let us get the unique description, a peculiar "formula" for every known way of committing such a kind of crimes. Implementation of such formalization will allow using many various mathematical methods for the exposure of the completeness and the consistency of the created classifications, the analysis of fundamental revealed criminalistic peculiarities and the prediction of potential ways of cybercrime commitment.

Corresponding Author:
Dr. Tatarinova Lola Furkatovna

7/22/2014

"Turan" University. St.Street 16-18-18a, Almaty city, 050013, Republic of Kazakhstan

References

1. WTSA Resolution 50: Cyber security (Rev. Johannesburg, 2008). Date Views 02.06.2014 www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf.
2. ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008). Date Views 02.06.2014 www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf.
3. ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at. Date Views 02.06.2014 www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf.
4. Dolgovoy, M., 2005. Criminology. M.: Norma, pp: 912.
5. Gaykovich, V. Yu. and A.P. Pershin, 1994. Electronic bank system security. M.: United Urope, pp: 360.
6. Kolisnechenko, A.N., 1973. Theoretical problems of crime investigation methodology. Issues of criminalistic methodology, tactics and investigation methods. M., pp: 76-79.
7. Vozgrin, 1993. I.A. Scientific bases of criminalistic methodology of crime investigation. Part IV. St. Pt.: St. Petersburg law university of MFA of Russia.
8. Belkin, R.S., 1997. Criminalistics course. In 3 Vol.: Criminalistic means, methods and recommendations. M.: Urist, pp: 537.
9. Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime. 2005. Date Views 02.06.2014 www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.
10. Convention on Cybercrime. COETS 8 (23 November 2001). Convention on Cybercrime. Budapest, 23.XI.2001. Date Views 02.06.2014 /www.worldlii.org/int/other/COETS/2001/8.html.
11. Joint Pub 3-13.1 "Command and Control Warfare", DOD US, February 1996.