Міжнародний юридичний вісник: збірник наукових праць Національного університету державної податкової служби України. Вип. 1 (1) 2014

UDC 344.1

N.S. Kozak,
Ph.D in Law, Assistant Professor,
National University of the State Tax Service of Ukraine

CRIME IN THE AREA OF COMPUTERS, COMPUTER SYSTEMS, COMPUTER NETWORKS AND TELECOMMUNICATION NETWORKS: CRIMINAL LEGAL ANALYSIS

У статті аналізуються об'єкт, об'єктивна сторона, суб'єкт, суб'єктивна сторона та особливості кваліфікації злочинів, передбачених статтями 361–363[1] Кримінального кодексу України.

Ключові слова: *комп'ютерні злочини, комп'ютерна інформація, інформаційні технології, злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, кримінально-правовий аналіз.*

This article covers the analysis of the object, the objective aspect, the subject and the subjective aspect of the specific features as to determination of the nature of crimes provided for by Articles 361–363[1] of the Criminal Code of Ukraine.

Keywords*: computer crime or cybercrime, computer information, information technology, crime in the area of computers, computer systems, computer networks and telecommunication network, criminal legal analysis.*

The crimes pertaining to using computers, computer systems, computer networks and telecommunication networks are referred to as the so-called computer crime or cybercrime.

The range of the scientists' viewpoints from extended understanding of computer crime that include all acts committed with the use of information technologies to the point that those computer related are the acts that are punishable under Section XVI of the Criminal Code of Ukraine [5].

The relevancy of criminal and legal analysis of the crimes provided for by Articles 361–363[1] of the Criminal Code of Ukraine is determined by the situation where the specific features of the language used in these clauses of the Criminal Code of Ukraine in a certain extent make it difficult and in some instances make it practically impossible to apply them, cause their ambiguous understanding by the officers of law enforcement and judiciary authorities, misclassification of crime, etc.

Analysis of the elements of the crimes provided for by Articles 361–363[1] of the Criminal Code of Ukraine in current wording was performed by such scientists as D.S. Azarov, A.S. Bilousov, V.M. Butouzov, M.V. Karchevsky, S.A. Kuzmin, A.A. Musika, M.V. Rudyk, V.P. Shelomentsev and others.

This research is performed with a view to define the optimal criminal and legal characteristics of crime in the area of using computers, computer systems, computer networks and telecommunication network.

The scientists' attention was once focused on the analysis of the following issues:

1) the law-maker's approach to criminalization of computer crime (in this case considering the varieties of these offences and the most common ways of commission of such crime, provisions of international legal acts ratified by Ukraine in the area of information, etc.);

2) problems lying in definition of the elements of the crimes provided for by Articles 361–363[1], Section XVI of the Criminal Code of Ukraine and this Section's heading;

3) ways to improve the provisions on the responsibility for these crimes (due to the reason that a lot of drawbacks were exposed with respect to conceptual framework, inconsistencies of the articles, scrappiness in their construction, drawbacks of Articles 361 and 362 of the Criminal Code of Ukraine, uselessness of Article 361[1] of the Criminal Code of Ukraine, excessive competition of the provision, for instance, between Articles 361[2] and 362 the Criminal Code of Ukraine, etc.);

4) ways to improve the structure of the Criminal Code of Ukraine (in particular, possibility of placing fraud committed by illegal operations with the use of computer technology (Part 3, Article 190 of the Criminal Code of Ukraine), use of fake electronic access facilities to bank accounts (Article 200 of the Criminal Code of Ukraine) and some other crimes to Section XVI of the Criminal Code of Ukraine), etc.

According to the existing in science criminal law approach the object of crime is divided into 'vertically' by general, generic (specific) and direct. Some authors notice about the division of the object 'horizontally' into basic, additional and optional [1, p. 44].

The general object of the crimes provided for by the Articles 361–3631 of the Criminal Code of Ukraine includes the aggregation of public relations as an integral system that guarded by the criminal law. Information relations and information security have rather important meaning in the aggregate of public relations of modern type of the state [7]. Information relations according to Law of Ukraine 'On Information' take place in all areas of life and activity of the society and the state in the course of information receipt, use, distribution and storage.

The generic object of these crimes is defined by the scientists, in particular, as regulated by law public relations of the automatic information processing (in particular, ensuring information processing security) [2, p. 21]; information relations supported by computers, computer systems, computer networks and telecommunication networks [4, p. 28]; public relations in the area of computer information that meaning lies in effecting of legal information activities by the party to relations with respect to the subject of these relations and obligations of the other participants not to impede it [1, p. 266].

In general it is possible to agree with the indicated above since the generic object should specifically be the information relations in the area of computer information along with the provision for protection of the persons' interests rather than any information relations.

In literature active discussion is under way on direct object of crimes provided for by Articles 361–363[1] of the Criminal Code of Ukraine. It is stated, in particular, that the main direct object means the following: normal operation of computers, automated systems, computer networks and telecommunication networks, their operating procedures (Article 361 of the Criminal Code of Ukraine); normal operation of the specified hardware (Articles 361[1], 363[1] of the Criminal Code of Ukraine); established operating procedures of computers, automated systems, computer networks

and telecommunication networks (Article 363 of the Criminal Code); property right to computer information (Article 361^2 of the Criminal Code of Ukraine) [1, p. 47, 52].

The approach of the researchers who place their emphasis on the property right to computer information is convincing due to the reason that the main element of the social danger of this crime is information value; the damage caused by unauthorized intrusion is not resulted from computer hardware, security, its procedure for use or telecommunication network operating security but from the information that is processed by the computer, computer systems, computer networks and the information received or transmitted by telecommunication networks [4, p. 54, 127].

The point is worthy of attention that relations in the area of are notably wider than the relations as to the property related to it; these crimes impede realization of the right to perform legitimate informative activities not only for the owner but also for the other persons (authorized users) who have the right, for example, to familiarize themselves with the information, to receive, to collect, to use it, etc. [1, p. 53, 54]. The direct object of these crimes is divided into the following: a) basic, which means specific public relations in the area of computer information that have emerged and exist due to performance of information activities by the certain person (or the persons) related to computer information, and those damaged substantially by the specific crime or those jeopardized by infliction of this damage; b) additional, which means the relations of property in computer information; c) optional, which means the public relations in the area of which the information activities are performed with respect to computer information [1, p. 266].

The direct object of the crimes provided for Articles 361–363^1 of the Criminal Code of Ukraine is normally taken to mean the information relations in the area of computer information, that is to say, the relations resulting from implementation of the information processes (creation, collection, processing, storage, search, transfer, output and distribution of computer information, the rights of the parties participating in the information processes) [5].

Speaking about the target of these crimes, it should be indicated that some authors, probably, judging by the heading of Section XVI of the Criminal Code of Ukraine, include to their list computer information, computer viruses, corresponding software and hardware as well as computers, automated systems, computer systems, computer, computer information carriers [7].

Notwithstanding the fact that traditionally the target of crimes is taken for any article of material world by which or by action (influence) on which the crime is committed, it is reasonable to agree with the proposal of the scientists related to expansion of the study about the target of crimes taking into account modern development trends of public relations and information society (so that this notion cover not only the articles but also the other objective material formations) [1, p. 266].

Accordingly, the target of these crimes, in the first place, shall be computer information as well as bad software and hardware designed for unauthorized intervention in the operation of computer, automated system, computer networks or telecommunication networks (under Article 361^1 of the Criminal Code of Ukraine. The information that is transmitted via telecommunication networks can be the target of these crimes only if computer information from one computer network to the other is transmitted via these networks [1, p. 103, 104; 4, p. 58]. It is obvious that computer, computer networks, automated systems, information media should be defined as the targets of crimes against property.

The specific feature of the crimes provided for by Articles 361–363^1 of the Criminal Code of Ukraine is that they are committed commonly by active actions. Crime provided for by Article 363 of the Criminal Code of Ukraine can be committed by action or omission. The components of the

crimes provided for by Articles 361, 362–363[1] of the Criminal Code of Ukraine are made as material and the rest of them as formal. The character of crime consequences and their rate depend on characteristics of the act and on the circumstances where it is committed.

As practice shows, information technology is the main tool for these crimes perpetration [5].

As a result of the scientific papers analysis as to components of the crimes provided for by Articles 361–363[1] of the Criminal Code of Ukraine we systemized the specific types of computer crimes inflicting severe damage to individuals, businesses though none of these articles provide for the responsibility for perpetration of these crimes. They include the following:

- access to computer information without protection penetration; actions that caused the consequences specified in Article 361 of the Criminal Code of Ukraine, if they were not proceeded by unauthorized intrusion in operation of the information processing resources (for example, powerful electromagnetic radiation effect); familiarization with the information processed in computers, automated systems, computer networks or telecommunication networks without the fact of unauthorized intrusion (with regard to Article 361 of the Criminal Code of Ukraine);

- creation, distribution and sale of the software not intended for unauthorized intrusion and harmful properties of which can show up without intervention in operation of computer (computers), automated systems, computer networks or telecommunication networks, in particular, this is about computer viruses (with regard to Article 361[1] of the Criminal Code of Ukraine);

- sale or distribution of restricted data that was created with violation of the applicable law; sale or distribution of restricted data that was received from protected computer network by protection system penetration but at the time of distribution this information was not protected already by the special hardware, for example, illegal distribution of electronic databases containing personal data (with regard to Article 361[2] of the Criminal Code of Ukraine);

- information interception in the course of the information transmission via telecommunication networks; illegal information output to computer (computers), automated systems, computer networks or telecommunication networks (with regard to Article 362 of the Criminal Code of Ukraine);

- distribution of the so called SPAM (due to the reason that these acts do not disrupt or shut not down computer (computers), automated systems, computer networks or telecommunication networks); mass distribution of the signals that do not contain any specific information for anyone by telecommunication networks resulted in malfunction or shut down of computer (computers); the act causing distortion of data processing (with regard to Article 363[1] of the Criminal Code of Ukraine).

In addition, no rules within any company, agency or organization governing operating procedures for computer, automated system, computer networks of telecommunication networks and the rules and the procedures for protection of non-state information exclude the presence in the persons acts of the component of crime provided for by Article 363 of the Criminal Code of Ukraine [1; 4].

The subjects of the crimes being analyzed can be punishable physical persons who reached the age of 18 at the moment of perpetration of the crimes. The special subject referred to above in two cases: the person who has the right for access to information (Article 362 of the Criminal Code of Ukraine); the person who is responsible for computers, automated systems, computer networks or telecommunication operation (Article 363 of the Criminal Code of Ukraine). The of the other crimes is general (the persons who has no right for access to computer information).

The scientists interpret the subjective side of the crimes differently. Generally, the authors define it in the following way: characterized by direct intent and commonly by mercenary motive;

the purpose is indicated in Article 361[1] of the Criminal Code of Ukraine; the act provided for Article 363 of the Criminal Code of Ukraine can be performed both intentionally and negligently, the attitude to violation of rules can be intentional (though there is the point that the act can be performed in the form of negligence only) [1, p. 201; 2, p. 28].

There is one more inconsistency in the analysis of the subjective side of the crime provided for by Article 362 of the Criminal Code of Ukraine. Some scientists denote the presence of guilt in the form of intention and negligence and the expediency to abolish the criminality of these negligent acts [1, p. 201] while the others denote direct or indirect intent [4, p. 86].

Qualifying elements of crime constitute commitment of the second crime or return to crime in collusion with the group of persons as well as commitment of crime that caused extensive damage. In literature there is a recommendation to the legislator to revise the provisions of articles indicated above with respect to return to crime, severe consequences, etc. [1, p. 157–161; 4, 123, 37–42].

Obviously, it is reasonable that the Supreme Specialized Court of Ukraine for Civil and Criminal Cases adopt the corresponding clarifications on such issues as interpretation of the terms, criminal and legal characteristics, the special features of crime qualification in the area of using computers, computer systems, computer networks and telecommunication networks, etc.

In this case heightened social danger of these crimes should be taken into consideration. Encroaching on the information relations the criminal causes damage or will try to cause damage to the relations to be intensified by information technology. We mean the crime having the target to the restricted data of different type, for instance, privacy of a person, medical, state secret, etc.

The specific character of the person's acts qualification is especially noteworthy as to the person who used information technology as the tool for perpetration of crime. It is essential to agree with the opinion of the scientists who denote that determination of the nature of the person's acts will be performed differently, in one instance as the crime provided for by one of the articles of Section XVI of the Criminal Code of Ukraine and in the other instance as the crime provided for by the article of the other section of the Criminal Code of Ukraine or as the aggregate of crimes [1, p. 134, 150, 197, 244, 248; 4, p. 29, 102–120]. Thus, intentional infliction of extensive damage resulted from destruction of the certain information that is important for the country's defense capacity with the purpose to weaken the country should be qualified as subversion (Article 113 of the Criminal Code of Ukraine) but not as unauthorized intrusion in that caused extensive damage (Part 2, Article 361 of the Criminal Code of Ukraine [4, p. 42].

A proposal to include in the list of the circumstance that aggravate the punishment such element of crime as 'commitment of crimes with the use of computer technology facilities' is convincing [3; 4].

Taking into account possibility of excessive competition of the legislative provisions, overlap the provisions of the Criminal Code of Ukraine due to incidence of the specific crimes determined nature as well as negligent attitude of the law-maker to social danger of crimes provided for by Articles 361–363[1] of the Criminal Code of Ukraine we consider this proposal as practical. It should be also noted that the 'situation is unacceptable where the crimes having different degree of criminal act provide for penalties of different types and at the same time the penalty for one type of crime is fixed in the similar amount of penalty and the amount of the other penalties differs substantially' [1, p. 212, 217].

If the act is qualified under the aggregate of crimes, probably, it would be reasonable not to use the circumstance that aggravates the punishment and not to take it into account in those cases

where in classified crime the point is about the information in electronic format (for instance, as it is provide for by Part 2, Article 301 of the Criminal Code of Ukraine).

It is reasonable to refine on the wording of this thesis, particularly, as follows: 'perpetration of the crimes with the use of information technologies' due to the reason that the term 'computer technology facilities' does not cover all possible computer-aided tools that are used for perpetration of crimes'.

In this context, implementation of the UNO Anti-Cybercrime Recommendations is perspective. In particular, this concerns development of the technology aimed at cybercrime prevention and investigation of up to development of the technologies directed on prevention and investigation, participation in determination of the priorities and the ways dealing with the problems in legislative are, holding of consultative events, workshops, seminars, edition of the literature on the issues that require resolution [6].

REFERENCES

1. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): [монографія] / Д.С. Азаров. – К.: Атіка, 2007. – 304 с.

2. Бутузов В.М. Науково-практичний коментар до Кримінального кодексу України. Особлива частина. Розділ XVI. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку / Бутузов В.М., Кузьмін С.А., Шеломенцев В.П. – К.: ПАЛИВОДА А.В., 2010. – 152 с.

3. Голина В.В. Проблемы компьютерной преступности / В.В. Голина, В.В. Пивоваров: матеріали міжнар. наук.-практ. семінару [„Фінансова злочинність"] / Національна. юридична академія України ім. Я. Мудрого, Департамент юстиції США; [ред. В.І. Борисов], (12–13 лютого 1999 р.). – Х.: Право, 2000. – С. 62–73.

4. Карчевський М.В. Злочини у сфері використання комп'ютерної техніки: [навчальний посібник] / М.В. Карчевський. – К.: Атіка, 2010. – 168 с.

5. Козак Н. Криміналістичні аспекти поняття „комп'ютерні злочини" / Н. Козак // Підприємництво, господарство, право. – 2013. – № 2. – С. 40–43.

6. Меры по борьбе против преступлений, связанных с использованием компьютеров : справочный документ семинара-практикума A/conf.203/14 / Одиннадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию, (Бангкок, 18–25 апреля 2005 года) [Электронный ресурс]. – Режим доступа: http://www.un.org/russian/events/ 11thcongress/ documents.html.

7. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: дис. … канд. юрид. наук: 12.00.09 / Мотлях Олександр Іванович. – Київ, 2005. – 198 с.

Подано до редакції 2 червня 2014 р.