International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 5 Issue 1, January - 2021, Pages: 80-87

Legal Legislative Basis for Detection of Information Crime

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Current social developments, the transition to electronic control of technological processes, the legalization of computer-generated acts have also created the conditions for the use of these processes to commit crimes in the field of information technology. Unlawful interference with the operation of components of telecommunications networks, computer programs operating in their environment, illegal modification and destruction of computer information can disrupt the work of extremely important elements of public infrastructure and lead to the loss of many lives and significant property damage. delivery or other socially dangerous consequences.*

Keywords: general object, special object, cognate object, direct object.

INTRODUCTION

1. Foreign experience in the field of information crime detection

2. Legal framework for the detection of information crime

The current realities of social development, the transition to electronic control of technological processes, the legalization of computer-generated acts have created the conditions for the use of these processes to commit crimes in the field of information technology. Unlawful interference with the operation of components of telecommunications networks, computer programs operating in their environment, illegal modification and destruction of computer information can disrupt the work of extremely important elements of public infrastructure and lead to the death of many people, significant property damage delivery or other socially dangerous consequences.

In the early stages of the development of network technologies abroad, the damage from viral and other types of computer attacks was small, as the economy was less dependent on information technology. At a time when the number of such attacks is growing, their automation mechanisms are being created, and citizens, businesses and public authorities are heavily dependent on electronic means of information use and exchange, the damage from attacks on information systems is enormous. amounts.

METHODS

The increase in crimes in the field of computer technology, their high level of social danger, necessitated the development of measures to protect against these crimes (primarily through the protection of computer technology itself). Research shows that 60% of such protections are legal, 20% cryptographic and 20% software, hardware and other physical and organizational means.

The first laws on computer technology in the United States in 1965 and the first criminal liability for computer abuse in Sweden in 1973 and the United Nations in 1994 on the prevention and control of computer-related crimes. the router was adopted.

The issue of legal regulation and protection of relations in the field of information technology in Uzbekistan began to be addressed in the early 90s of last century. This delay was partly due to the low level of computer development in our country.

On May 6, 1994, the Law of the Republic of Uzbekistan "On legal protection of programs and databases created for computers" was adopted. It was later amended by the laws of the Republic of Uzbekistan of April 5 and August 8, 2002. The law deals with administrative and criminal liability (Article 15) and provides for liability for copyright infringement. Adoption of the Laws of the Republic of Uzbekistan "On Principles and Guarantees of Freedom of Information" of December 12, 2002 and "On Informatization" of December 11, 2003 is the basis of the legislation on combating crimes in the field of information technology is formed. They define many legal and technical terms that are of fundamental importance for the proper classification of crimes and the prosecution of perpetrators.

Crimes in the field of information technology not only violate the inviolability of intellectual property, but also the disclosure of information about the privacy of citizens, property damage in the form of direct damage and unearned profits, defamation of the firm, violation of the legal activities of enterprises, institutions and organizations. different species and so on.

Based on the above these types of crimes encroach on relationships that ensure the lawful, secure use of information technology.

Based on the theory that the object of the crime has a four-tiered structure, the common object of criminal aggression related to the illegal use of information technology is the whole set of social relations protected by criminal law, special ob. The act consists of a set of social relations on public safety and public order, the legal and safe use of information technology in a related object. The direct object is determined by the name and disposition of a particular substance. In most cases, this type of object of the main component of the crime in the field of information technology is expressed in an alternative way, and in aggravating elements, their number is naturally increased.

The separation of general, special, related and direct objects objectively reflects the whole scope of social relations, which are the object of criminal law protection, and corresponds to the current structure of the Criminal Code of the Republic of Uzbekistan11.

The subject of information technology crimes is still controversial. In particular, there are different opinions in the legal literature about the object and subject of this type of crime. For example, VV Krylov believes that the object of these crimes is computer data12. L. Chichko said that an object means computer information13, and V.B. Vekhov meant machine information14. Proponents of the idea that information can be the subject of a crime believe that information, including computer information, is a convenience created for society, so it is true that it can be damaged if it is illegally destroyed or modified. However, computer information (such as classified information) may be illegally copied and blocked. The information itself is not harmed. However, the object of the crime is always the victim of the crime, otherwise there is no corpus delicti. So what is crime? What happens in the above two cases? What does it hurt and how?

In the first case, the relationship of monopoly use of the legal owner of the information is harmed, and in the second case, the relationship of direct legal and safe use is harmed. Therefore, it can be concluded that computer information does not always harm itself, but in all cases, the relationship between its use is broken.

In criminal law, computer information is the subject of crimes in the field of information technology. For example, such cases are directly reflected in the provisions of Articles 2781, 2782, 2784 and 2786 of the Criminal Code. In other cases

11 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

12 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

13 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

14 See Vexov V.B. Computer prestupleniya: sposoby sovershеniya i raskrytiya. - M., 1996. –S.163.

the identification of the subject is related to the identification of other elements of the crime (Articles 2783 and 2785 of the Criminal Code).

In accordance with Article 3 of the Law of the Republic of Uzbekistan "On the Principles and Guarantees of Freedom of Information", information refers to persons, things, facts, events, events and processes, regardless of the form of presentation the data is understood. The peculiarity of the chapter on information technology crimes in the Special Part of the Criminal Code is that it deals with a special type of information - computer information.

Computer information is computer programs and databases that are processed and used by a computer and contain information about persons, objects, facts, events, happenings and processes, as well as the owner's identification attributes that define the mode (rules) of its use. Computer programs and databases should also be protected from criminal law. Here are the features of computer programs. They are, on the one hand, a means of influencing information and, on the other hand, information consisting of commands and data sets. That is, they have a certain duality. This is the basis for interpreting a computer program as a type of information. Article 1 of the Law of the Republic of Uzbekistan "On legal protection of computer programs and databases" defines computer programs as follows: "Computer software - an objective form of representation of a set of data and commands designed

to operate a computer and other computer devices in order to obtain a specific result. The computer program includes the preparatory materials received during its development, as well as the audiovisual images produced by this program.

So what is a database? According to the above law, "a database is an objective form of presentation and organization of a set of data, arranged in such a way that this data can be found and processed by computer (e.g., items, calculations).) ».

As you know, computer information can be on a carrier, on a computer, on a computer system, on a computer network.

A carrier is a device designed to permanently store and transport computer information.

A computer consists of a system unit that includes a microprocessor, a keyboard (a device that allows you to enter typed characters into a computer), and a monitor (a device that displays various information).

Various peripherals can be connected to the computer's system unit. They are designed to expand the functionality of the computer. Such devices include printers, scanners, modems, etc. The computer system consists of the computer itself and all the surrounding devices.

A computer network is a combination of several computers created by special cables.

The legal literature sometimes raises puzzling questions about such information technology-related crimes. For example, when a computer is used to commit another unlawful attack on another object, can computer information be the sole object or means of the crime? The Russian scientist AV Sorokin answers: "Acceptance of information as a tool in the commission of other crimes

"In overstating the scope of the concept of 'computer crime' and complicating the work of both the legislature and the law enforcement agencies."

From a technical point of view, computer information is indeed a means of action within a computer system (not necessarily a criminal act), but we must not separate it from the computer itself. Simply put, information is not a separate thing from a computer, but a technical and legal tool. Therefore, in qualifying crimes committed by exposure, the issue can also be considered over. To do this, the computer can be understood as a complex of hardware and software. When a payment is made for a purchase using a fake plastic card, or when money is transferred from one bank account to another illegally or unpaid, the act must be considered a form of robbery.

The objective aspect of the content of crimes in the field of information technology is often expressed as material. Therefore, not only the occurrence of a socially dangerous act, but also the occurrence of socially dangerous consequences, as well as the identification of the causal link between the act and the consequence is considered. The separate components of crimes (Articles 2783 and 2786 of the Criminal Code) are defined in the law as a formal component. When they end, they indicate the time at which the action or inaction occurred, regardless of when the consequences occurred. Socially dangerous acts themselves take the form of actions applied to these crimes, and can sometimes be inaction. In one case, such a sign of the objective side of the crime is expressed as a method of committing the crime, as a mandatory sign of the elements with the main and aggravating circumstances. In other cases, the nature of the crime, as well as the place, time, weapons, means, and circumstances of the crime, may be considered by the court as mitigating or aggravating circumstances.

Crimes in the field of information technology are committed using various computers, hardware, peripherals and communication lines. This, in turn, raises the question of where the crime took place. The creation of the World Information Network (INTERNET), which unites representatives from almost all countries of the world, will allow to do things far from the place where the harmful consequences will occur. In such cases, Russian researchers YU. I. Lyapunov and A. V. Pushkin, when we say the place of the crime, understand the territory of the state where the act (action or omission) took place, regardless of where the consequences occur. In resolving the issue in this way, the authors argue that Article 9, Part 2 of the Criminal Code of the Russian Federation stipulates that the time of the act is the time of the crime, regardless of when the consequences occur. anadilar16. However, without making the necessary clarifications to the above provision, it cannot be adopted into the criminal law of the Republic of Uzbekistan, as it contradicts Article 13 (1) of the Criminal Code of the Republic of Uzbekistan. According to this article, the time of the crime is determined by what (formal or material) crime was committed. The time of the commission of a formal crime should be recognized as the time of the commission of a socially dangerous act, and the time of the commission of a material crime should be recognized as the time of the occurrence of criminal consequences under criminal law17. Therefore, the place of commission of formal crimes in the field of information technology is the territory of the state where the socially dangerous act was committed, and the place of commission of material crimes is 15 See Sorokin A.V. Computer prestupleniya:

ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

16 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

17 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

the territory of the country where the consequences occurred (information was destroyed, modified, blocked, copied).

The subjective aspect of information technology crimes is characterized by a direct or indirect form of guilt. Only one crime, that is, the crime under Article 2781 of the Criminal Code, which establishes liability for violation of the rules of information, can be committed both intentionally and through negligence.

For two offenses by the legislature, Articles 2783 and 2786 of the CC set the goal as a necessary feature of the subjective side of the crime. In other cases, motive and purpose are not specified as necessary signs of crimes, but their definition is important for the individualization of punishment. These crimes can be committed out of greed, hooliganism, revenge, "in the interests of sports", as well as political and other interests. This type of crime can be committed for purposes such as striving for supremacy, desire for pleasure, concealment of other crimes.

The subject of information technology crimes is a sane person who has reached the age of 16, has a duty to protect information, or has illegally accessed computer information.

From the point of view of psychophysiological description, they are a creative person, a specialist, able to take the risk of a technical call. Today, large companies are trying to hire experienced hackers to create a system of protection for information and computer systems.

According to expert research, 33% of those under the age of 20 at the time of the crime, 54% of those aged 20-40, and 13% of those over 40 were involved in crime. The study refutes the assumption that hackers are teenagers between the ages of 13 and 20.

Men are up to five times more likely to commit computer crimes. The majority of such offenders have higher or incomplete higher technical education (53.7%), while the rest have higher education, as well as incomplete higher education (19.2%).

The number of women in their ranks has been growing recently. This is largely due to the fact that women (secretaries, accountants, economists, managers, treasurers, supervisors, etc.) occupy many jobs, specialties and positions related to computer equipment.

Criminological research shows that 52% of offenders have special training in computer information processing; 97% are employees of government agencies and institutions that use computer systems and information technology in their daily work; Thirty percent are offenders directly involved in the operation of computer equipment18.

In conclusion, the range of individuals who commit crimes in the field of information technology is relatively wide. The results of the study show that the subjects of crime can be people from all walks of life, from 16 to 60 years, and the level of training - from inexperienced to professionals or people of all ages with minimal knowledge in the field of computer technology.

18 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost za nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

Based on the analysis of objective and subjective characteristics, these crimes can be described as follows: computer r. In the field of information technology, a socially dangerous act that harms or threatens to harm social relations in the legal and safe use of information, which is punishable, is called a crime in the field of information technology.

The social risk of crimes in the field of information technology is significantly increased in the following cases: a) by a group of individuals with prior conspiracy; b) by a repeat and dangerous recidivist; c) by an organized group or in its interests; g) caused a large amount of damage.

Such necessary signs are contained in paragraphs "a" and "b" of all types of crimes in the field of information technology, except for the crime specified in Article 2781 of the Criminal Code. The commission of a crime by an organized group or in its interests is

a qualification mark of the second part of Articles 2782, 2783, 2786 of the Criminal Code. Causing excessive damage is a qualification mark of the second part of Articles 2781, 2784, 2786 of the Criminal Code.

According to Article 29 § 3 of the Criminal Code, a crime is said to have been committed by a group of persons with prior conspiracy to commit a crime jointly by two or more persons. In the field of information technology, a conspiracy to commit a crime means that the objective aspect of the crime occurs before the execution of the signs or as a result of a sudden intention, directly before the execution.

Pre-conspiracy in a joint act or participation means, in a narrow sense, the division of responsibilities in the commission of a crime (executor, assistant, witness, organizer), as well as the fact that all members of the group conspired to commit a crime with subjective characteristics.

If one member of a group is a subject of a crime and the others are not considered a subject because they are minors, a group with which they have previously conspired is considered non-existent. In this case, the sole subject has committed crimes in the field of information technology, as well as for inciting minors to engage in antisocial behavior (Article 127, part 3 of the Criminal Code) if he incited minors to commit crimes. will be held accountable for the set.

It should be noted that the person who is the subject of the crime forced the juvenile to commit a crime, and if he did not participate in it, he was charged with using the juvenile as a weapon. will be held accountable as the executor. According to Article 32 (1) of the Criminal Code, recidivism means that a person has committed two or more crimes provided for in different articles at different times, but not for any of them, in cases specified in the same article, part or Code of the Special Part of the Criminal Code. not convicted.

However, it does not matter whether the previous offense has been completed or whether the offender has committed the offense as a perpetrator or other type of complicity. Repetition in information technology crime consists of two or more similar crimes.

This means that a repeat offender has committed a similar (similar) socially dangerous aggression. For example, computer sabotage is committed by a person for the second time and if the first act contains elements of a crime under part 1 of Article 2785 of the Criminal Code and is not prosecuted (Article 2785, part 2, paragraph "b"), then repeated is committed. How much and in what form is the crime committed?

regardless of whether The main thing is that a similar crime committed before should have retained its legal significance under Article 64 of the Criminal Code.

According to Article 34 § 2 of the CC, a dangerous recidivist is defined as an intentional new crime committed by a person who has committed a crime similar to a previously convicted crime. In order to qualify information technology crimes as committed by a dangerous recidivist, law enforcement agencies are obliged to bring charges against the perpetrator, taking into account this sign. If a person is previously convicted of illegal (unauthorized) use of computer information specified in part 1 of Article 2782 of the Criminal Code and commits a similar crime again, according to Article 2782, part 2, item "b" of the Criminal Code (as a dangerous recidivist) should be prosecuted.

It should be noted that the main condition for taking into account the necessary criteria in the qualification of these crimes is the fact that the term of execution of the sentence (Article 69 of the Criminal Code) has not expired or the conviction has not been completed in accordance with the law. whether or not the person has been convicted of a similar crime in the past.

An organized group is a group of two or more persons who have previously joined a group to carry out criminal activities together (Article 29 § 4 of the CC).

The longevity of the group's criminal activity, the consistency of the composition, the strength of the relationship, the hierarchical distribution of roles and responsibilities (vertically and horizontally) between group members in the field of activity with other close groups through the leader (manager, organizer), criminal strict internal discipline in planning activities is described as the organization of a criminal group19.

The listed characters belong to this or that type of crime and are more or less present in any organized group. In addition, in order for a group to be considered organized, it is necessary to determine whether the group was set up to carry out criminal activities in the area of illegal and secure use of computer information.

Articles 2783 and 2786 (2) (g) of the Criminal Code stipulate the grounds, conditions and scope of criminal liability of persons who organized or led an organized group, as well as those involved in the group's crime. The word goes on. In such cases, all members of an organized group, regardless of their role in the commission of a particular crime, are prosecuted as perpetrators (without reference to Article 28 of the CC). The above-mentioned aggravating circumstance is defined as the qualification criteria in the articles of the Special Part of the Criminal Code, as it is determined that the crime was committed by an organized group or in its interests. According to them, a convicted person who is not a member of an organized group, but once participated in the commission of an organized crime or committed the crime independently, on his own initiative or by order of an organized group, in the interests of the organized group. also applies to individuals.

Article 2781, part 2, Article 2784, part 2, item “a” and Article 2786, part 2, item “a” of the Criminal Code provide for a large amount of damage equal to three hundred times the minimum wage and more. is equal to many. In this case, the concept of "loss" is not only the direct damage, but also the lost benefit. Separately

19 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.

it should be noted that as a result of the commission of a crime, a person has in fact caused less damage than a very large amount, but if the intention of the offender is aimed at causing such damage, the crime is classified as an assassination.

The criminal law of the Republic of Uzbekistan establishes liability for crimes with six main and qualifying components in the field of information technology.

RESULTS

According to Article 34 § 2 of the CC, a dangerous recidivist is defined as an intentional new crime committed by a person who has committed a crime similar to a previously convicted crime. In order to qualify information technology crimes as committed by a dangerous recidivist, law enforcement agencies are obliged to bring charges against the perpetrator, taking into account this sign. If a person is previously convicted of illegal (unauthorized) use of computer information specified in part 1 of Article 2782 of the Criminal Code and commits a similar crime again, according to Article 2782, part 2, item "b" of the Criminal Code (as a dangerous recidivist) should be prosecuted.

It should be noted that the main condition for taking into account the necessary criteria in the qualification of these crimes is the fact that the term of execution of the sentence (Article 69 of the Criminal Code) has not expired or the conviction has not been completed in accordance with the law. whether or not the person has been convicted of a similar crime in the past.

An organized group is a group of two or more persons who have previously joined a group to carry out criminal activities together (Article 29 § 4 of the CC).

The longevity of the group's criminal activity, the consistency of the composition, the strength of the relationship, the hierarchical distribution of roles and responsibilities (vertically and horizontally) between group members in the field of activity with other close groups through the leader (manager, organizer), criminal strict internal discipline in planning activities is described as the organization of a criminal group19.

The listed characters belong to this or that type of crime and are more or less present in any organized group. In addition, in order for a group to be considered organized, it is necessary to determine whether the group was set up to carry out criminal activities in the area of illegal and secure use of computer information.

Articles 2783 and 2786 (2) (g) of the Criminal Code stipulate the grounds, conditions and scope of criminal liability of persons who organized or led an organized group, as well as those involved in the group's crime. The word goes on. In such cases, all members of an organized group, regardless of their role in the commission of a particular crime, are prosecuted as perpetrators (without reference to Article 28 of the CC). The above-mentioned aggravating circumstance is defined as the qualification criteria in the articles of the Special Part of the Criminal Code, as it is determined that the crime was committed by an organized group or in its interests. According to them, a convicted person who is not a member of an organized group, but once participated in the commission of an organized crime or committed the crime independently, on his own initiative or by order of an organized group, in the interests of the organized group. also applies to individuals.

DISCUSSION

The increase in crimes in the field of computer technology, their high level of social danger, necessitated the development of measures to protect against these crimes (primarily through the protection of computer technology itself). Research shows that 60% of such protections are legal, 20% cryptographic and 20% software, hardware and other physical and organizational means.

The first laws on computer technology in the United States in 1965 and the first criminal liability for computer abuse in Sweden in 1973 and the United Nations in 1994 on the prevention and control of computer-related crimes. the router was adopted.

The issue of legal regulation and protection of relations in the field of information technology in Uzbekistan began to be addressed in the early 90s of last century. This delay was partly due to the low level of computer development in our country.

On May 6, 1994, the Law of the Republic of Uzbekistan "On legal protection of programs and databases created for computers" was adopted. It was later amended by the laws of the Republic of Uzbekistan of April 5 and August 8, 2002. The law deals with administrative and criminal liability (Article 15) and provides for liability for copyright infringement. Adoption of the Laws of the Republic of Uzbekistan "On Principles and Guarantees of Freedom of Information" of December 12, 2002 and "On Informatization" of December 11, 2003 is the basis of the legislation on combating crimes in the field of information technology is formed. They define many legal and technical terms that are of fundamental importance for the proper classification of crimes and the prosecution of perpetrators.

Crimes in the field of information technology not only violate the inviolability of intellectual property, but also the disclosure of information about the privacy of citizens, property damage in the form of direct damage and unearned profits, defamation of the firm, violation of the legal activities of enterprises, institutions and organizations. different species and so on.

CONCLUSION

Crimes in the field of information technology not only violate the inviolability of intellectual property, but also the disclosure of information about the privacy of citizens, property damage in the form of direct damage and unearned profits, defamation of the firm, violation of the legal activities of enterprises, institutions and organizations. different species and so on.

Based on the above these types of crimes encroach on relationships that ensure the lawful, secure use of information technology.

Based on the theory that the object of the crime has a four-tiered structure, the common object of criminal aggression related to the illegal use of information technology is the whole set of social relations protected by criminal law, special ob. The act consists of a set of social relations on public safety and public order, the legal and safe use of information technology in a related object. The direct object is determined by the name and disposition of a particular substance. In most cases, this type of object of the main component of the crime in the field of information technology is expressed in an alternative way, and in aggravating elements, their number is naturally increased.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

5 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

6 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

7 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

8 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

9 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

10 See Vexov V.B. Computer prestupleniya: sposoby sovershenіya i raskrytiya. - M., 1996. –S.163.

11 See Sorokin A.V. Computer prestupleniya: ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

12 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

13 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

14 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost for nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

15 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.