PROSECUTOR’S SUPERVISION OVER THE LEGALITY OF THE PRELIMINARY INVESTIGATION AND INQUIRY DURING THE QUALIFICATION OF CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Atobek Ravshanovich Davronov

Academy of the General Prosecution office, atodavr@gmail.com

Follow this and additional works at: https://uzjournals.edu.uz/proacademy

Part of the Criminal Law Commons, Criminal Procedure Commons, Human Rights Law Commons, Law and Economics Commons, and the Law Enforcement and Corrections Commons

Recommended Citation
Available at: https://uzjournals.edu.uz/proacademy/vol2021/iss1/1

This Article is brought to you for free and open access by 2030 Uzbekistan Research Online. It has been accepted for inclusion in ProAcademy by an authorized editor of 2030 Uzbekistan Research Online. For more information, please contact sh.ervin@edu.uz.
PROSECUTOR'S SUPERVISION OVER THE LEGALITY OF THE PRELIMINARY INVESTIGATION AND INQUIRY DURING THE QUALIFICATION OF CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Abstract: Correct, that is, consistent with the principles of criminal law and criminal law, qualification of a crime ensures accurate and full application of the complex of norms of criminal and criminal procedure laws. Depending on the qualification of the crime, criminal law issues are resolved about punishment, release from criminal liability and punishment, parole, calculation of convictions, amnesty. The qualification of crimes is important for initiating a criminal case, determining the subject of proof, ensuring the rights of the accused and applying other criminal procedural norms. This scientific and practical article is devoted to the prosecutor's supervision over the correct qualifications in the investigation of crimes in the field of information technologies and proposals are given for improving the criminal procedural law. Despite the recognition of the great social and legal significance of the qualification of crimes, as well as the scientific validity of the conclusion that the qualification of crimes as a form of law enforcement is subject to internal laws and rules, the problem of legal regulation of the rules for qualifying crimes in the field of information technology remains unresolved.

Keywords: code, investigation, prosecutor, violation, informatization, computer modification, malicious, programs legislators, illegal, telecommunication, networks, sabotage, distribution, electronic, selling, donating, renting, lending, transmission, mail.

Introduction

The subject of the qualification of a crime in a criminal case is a person who is authorized to make procedural decisions: the investigator, the head of the investigative body, the interrogator, the head of the inquiry body and the court. The prosecutor is also the subject of qualifying a crime in a criminal case, but unlike other law enforcement officers, his criminal-legal assessment of the act takes on more complex procedural forms.

Exercising supervision over the activities of the bodies of pre-investigation inspection, inquiry and preliminary investigation, the prosecutor assesses the correctness of the application of the criminal law at the stage of pre-trial proceedings, including the validity of the qualification of the crime.

In accordance with Art. 15 of the Criminal Procedure Code of the Republic of Uzbekistan, the prosecutor, investigator and interrogating officer are obliged, within their competence, to initiate a criminal case in each case of detection of signs of a crime, to take all measures provided for by the Criminal Procedure Code to establish the event of a crime, persons guilty of committing a crime, and to their punishment. At the same time, he is obliged not only to record such a fact, but also to give him an accurate criminal-legal assessment, i.e. to qualify the deed.

In addition, in accordance with part 3 of paragraph 3 of Article 382 of the Criminal Procedure Code of the Republic of Uzbekistan, exercising supervision over the implementation of laws by the bodies of inquiry and preliminary investigation, the prosecutor, within the limits of his competence, gives written instructions on the investigation of crimes, on the election, change or cancellation of a preventive measure to initiate a petition on the establishment of an additional prohibition (restriction) on house arrest, on the qualification of a crime, involvement in the case as an accused, the performance of certain investigative actions and the search for persons who have committed crimes. Based on this,
the prosecutor must pay attention to the correctness of the classification of crimes by the bodies of inquiry and preliminary investigation.

Despite the fact that the content of the qualification of a crime by a prosecutor cannot be different from what is required by a single law for all, the legal nature of the qualification carried out by a prosecutor differs from the similar qualification produced by an investigator, interrogator or court. According to Obrazhiev K.V., Pikurov N.I. the investigator, the interrogating officer and the court carry out qualifications in the process of applying the criminal law in the criminal case that is in their proceedings. They directly implement their decisions in procedural documents that determine the scope and legal restrictions of the accused (defendant). Unlike the court, which also does not depend on the departmental interests and interests of the parties to the criminal process, the prosecutor has the opportunity to use legal instruments to influence decisions of persons who directly apply criminal law and who qualify a crime at the stage of pre-trial proceedings. The qualification carried out by the prosecutor is embodied in the procedural act of the application of the criminal law through the requirements for eliminating violations of the law committed during the inquiry and preliminary investigation, which includes the requirement to correct the qualification error. In this case, there is a mistake in qualifying crimes in the field of information technology.¹

**Research methods.**

The research is based on modern scientific methods of jurisprudence and state studies, applied sociology, probability theory, computer science and management theory. When working on the dissertation, the author relied widely on the results of research by Russian and foreign legal scholars in the considered and related fields of knowledge.

The most important methodological basis of the study was a systematic approach to the problem of information bases for qualifying crimes. It allowed us to analyze the main stages and components of the information-analytical work of various subjects in the qualification process, their specific properties and features, to determine the ways of its improvement, to consider information support in this area as a system.

Information technology, which is the main wealth of society, is naturally the object of various types of criminal encroachments in the Republic of Uzbekistan. Among them a special role belongs to cybercrime, which domestic legislators are divided into seven types:

1. Violation of the rules of informatization (Art. 278¹ of the Criminal Code of the Republic of Uzbekistan);
2. Illegal (unauthorized) access to computer information (Art. 278² of the Criminal Code of the Republic of Uzbekistan);
3. Manufacturing for the purpose of marketing or marketing and distribution of special means for obtaining illegal (unauthorized) access to a computer system, as well as to telecommunication networks (Art. 278³ of the Criminal Code of the Republic of Uzbekistan);
4. Modification of computer information (Art. 278⁴ of the Criminal Code of the Republic of Uzbekistan);
5. Computer sabotage (Art. 278⁵ of the Criminal Code of the Republic of Uzbekistan);
6. Creation, use or distribution of malicious programs (Art. 278⁶ of the Criminal Code of the Republic of Uzbekistan);

---


**Article 278¹. Violation of the rules of informatization.**

According to the Criminal Code of the Republic of Uzbekistan, illegal (unauthorized) access to computer information, that is, information in information and computing systems, networks and their components, if this action entailed the destruction, blocking, modification, copying or interception of information, disruption of the operation of electronic computers, electronic computer systems or their networks.

When determining the composition of this crime, when checking the legality of the inquiry and preliminary investigation, the prosecutor needs to pay attention, but the fact that the object of violation of the rules of informatization is public relations to ensure the security of computer information (inviolability of computer information), as well as the procedure for using automated data processing systems. Public relations related to the protection of personal or property interests of citizens or state or public interests are used here as an additional direct object.

On the objective side, violation of the rules of informatization consists in the creation, implementation and operation of information systems, databases and data banks, information processing and transmission systems, authorized access to information systems without taking established protection measures, which caused major damage or significant harm to the rights or interests of citizens protected by law, either state or public interest.  

The subject of the crime under Art. 278¹ of the Criminal Code of the Republic of Uzbekistan, there may be a sane person who has reached the age of 16. The law does not require that this person be a specialist in the field of computer technology or engage in certain activities, the main thing is that he has access to information systems.  

The subjective side of the crime under Part 1 of Art. 278¹ of the Criminal Code of the Republic of Uzbekistan is characterized by:

- by intent, when a person realizes that he is violating the rules of informatization, foresees the possibility or inevitability of causing significant damage to the legitimate user as a result of this, wishes (direct intent) or deliberately allows these consequences to occur (indirect intent);
- negligence, when a person realizes that he is violating the rules of informatization, foresees the possibility of the onset of the consequences specified in the law, but unreasonably expects that they will not occur (criminal arrogance) or does not realize the socially dangerous nature of his act, does not foresee the onset of adverse consequences, although could and should have foreseen them (criminal negligence);
- a complex form of guilt, when in relation to the criminal act itself, i.e. violation of the rules of informatization, there is intent, and in relation to the adverse consequences provided for by law - negligence.

---


The motive and purpose for the crime are optional.

Under computer information in this crime Aisanov R.M. understands "intellectual property information recorded on a tangible medium or transmitted through telecommunication channels in a form available for its automated processing, storage and transmission, explicitly limited by the owner in its free use".\

Kopyryulin A.N. considers computer information as "an organizationally ordered set of information (messages, data) recorded on a machine medium or in an information and telecommunication network with details that allow them to be identified, having an owner or other legal owner".\

In this type of crime Rustambaev M. Kh. believes that under computer information it is necessary to understand here information about certain facts, persons, events, processes contained on a computer medium, in electronic computers, a system of electronic computers or their networks and available for processing using electronic computers.

According to V.N. Shchepetilnikov, the totality of social relations associated with the circulation of information cannot be exhausted by the use of the term computer, since it is only one of the varieties of electronic computers. In this regard, it is more expedient to talk about electronic information, since only computer information cannot be taken as the basis of criminal law protection.

Efremova M.A. under "electronic information" proposes to understand "information (messages, data) presented in electronic digital form, regardless of the means of storage, processing and transmission". At the same time A.V. Geller notes that electronic information can act as both a means of committing a crime and its subject in cases when it is recorded on a tangible medium in the form of an electronic document.

Under digital information S.P. Kushnirenko understands "any information presented in the form of a sequence of numbers available for input, processing, storage, transmission using technical devices." This definition seems to be not entirely successful, since it does not contain an indication of the way information is presented in such devices. For example, a simple combination of numbers is available for input using an ordinary typewriter. Obviously, the information presented in this way is not digital in the context under consideration.

Another definition is offered by I.R. Begishev. he understands digital information as "a set of information circulating in information and telecommunication devices, their systems and networks." The proposed definition should be recognized as successful, subject to the condition of a uniform understanding of the term "digital" as referring to the field of information technology. Only in this case, the refusal to indicate the method of presenting information can be considered appropriate.

---

5 Айсанов Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: автореф. дис. ... канд. юрид. наук. URL: http://www.dissercat.com/content/sostav-nepravomernogo-dostupa-k-kompyuternoi-informatsii-v-rossiiskom-mezhdunarodnom-i-zarube. [Aisanov R.M. Composition of unlawful access to computer information in Russian, international and foreign criminal legislation: author. dis. sciences.]


The Law "Informatization" uses another concept of an information resource, similar to the stated term, meaning information, a data bank, a database in electronic form as part of an information system[13].

Thus, based on the research conducted, the prosecutor, when checking the correct qualifications by the bodies of inquiry and preliminary investigation, under the computer information should understand electronic information, which includes information (messages, data) presented in digital form and contained in information and telecommunication devices, their systems and networks. This definition is not without its drawbacks, but it is able to most fully reflect the essence of the phenomenon under consideration. In any case, we hope that the proposed option will serve as an additional stimulus for continuing the scientific discussion.

In this corpus delicts, Rustambaev M.Kh. believes that machine information carriers are objects and devices that have physical properties (including physical fields) that allow you to capture, store and read information by means of electronic computing technology (these are magnetic disks that are either an integral part of electronic computers or an accessory its peripheral device, magnetic tape, storage floppy disk (floppy disk), CD, etc.).

According to Kuznetsov P.U. a kind of material medium of a document is a computer-readable medium, on which the recording of documented information is carried out in ways that ensure the processing of such information by an electronic computer[14].

According to Sokolov Y.N. An electronic storage medium is not just a material medium, but an electronic device complex in its internal structure, configuration and manufacturability with the following specific features:

- the material from which the carrier is made is capable of repeatedly storing, changing and reproducing the electronic information recorded on it, depending on the needs of the user or the purpose of the device;
- the presence of software, initially stored in the internal memory of the device, for visualization of the binary information available (recorded) on it, on a computer screen or the possibility of its transmission in accordance with transport protocols for data transmission over the unified telecommunication network of the Republic of Uzbekistan and international telecommunication networks consistent with it;
- providing the possibility of long-term storage of the recorded electronic information in the internal memory of the device (a feature of the material of the carrier performing this function, or the presence of additional (external or internal) energy sources capable of supporting this ability of the carrier);
- with the exception of the possibility of modifying the electronic information recorded (available) on the carrier, i.e. her safety. Security in this case should be understood not only in the aspect (threat) of changes and destruction of electronic information, but also unauthorized copying, i.e. illegal access to the content of an electronic data carrier;
- the possibility of separating the available electronic information from its possible analogs stored on similar media or information sources when the electronic media is connected to computer devices or information and telecommunications data transmission channels.

In this regard, from a scientific point of view, we agree with the opinion of Y.N. Sokolov, which claims that an electronic storage medium should be understood as an electronic device technically and technologically adapted to multiple use, intended for recording, storing, transmitting and reproducing electronic information using available technical means, as well as protecting, separating and delimiting access to available information[15]. The prosecutor, when checking the correct qualification of the corpus delicts by the bodies of inquiry and preliminary investigation, must pay attention to this concept.
The legislator did not give a definition of the concept of "computer", which put the law enforcement officer in a position where in each case it is necessary to consider the properties of a particular device and decide whether to recognize or not recognize its computer and, accordingly, to bring a person to criminal liability or not.

Rustambaev M.Kh. adheres to the opinion of Krylov V.V. that under electronic computers it is necessary to understand "a complex of electronic devices that allow performing operations prescribed by the program and/or the user (sequence of actions for processing information and controlling devices) on symbolic and figurative information, including its input-output, destruction, copying, modification, transmission of information in the network of electronic computers and other information processes"[16].

Electronic computers should also include the so-called integrated systems (computers in an unconventional sense - cell phones, pagers, electronic cash registers, electronic ATMs and terminals for working with plastic payment cards).

So, in particular, a cellular telephone network can be considered as a computer network, the components of which are cellular telephones, base stations, a switch and a controller. At the same time, the cellular device itself, being a microprocessor device, acts as a remote workplace of the wireless network, and the central controller acts as a file and communication server. The entire system of operation of such a network is based on computer technology and the exchange of information between the central computer (controller, switchboard) and peripheral installations (cellular telephones).

The paging network can be viewed in a similar way, with the only difference that the pager is a remote terminal. Due to this, the articles of chapter XX¹ of the Criminal Code "Crimes in the field of information technology" apply to information located in cellular and paging networks[17].

According to N.I. Vetrov, Y. I. Lyapunov, an electronic computer is a complex of technical means designed for automatic processing of computer information in the process of solving computational and information problems[18].

Mazurov V.A. believes that an electronic computer is a set of electronic devices, the basis of the functioning of which is a descriptive model of an infinite automaton, allowing to perform operations prescribed by the program and (or) the user on computer information, including its input-output, destruction, copying, modification, transmission of information in the computer network and other information processes[19].

According to Pashin S.A. an electronic computer is a computer that converts information in the course of its functioning into numerical form[20].

The prosecutor, when checking the correct qualification of the corpus delicti by the bodies of inquiry and preliminary investigation, must pay attention to the fact that under electronic computers this is a device consisting of hardware and software, functionally and exclusively intended for processing and transforming information, that is, for performing operations with information (information) presented in electronic digital format, devoid of any household function. The prosecutor, when checking the correct qualification of the corpus delicts by the bodies of inquiry and preliminary investigation, must pay attention to this concept.

A computer system (computer system, information computer system, computer system) is “a set of interconnected and interacting processors or electronic computers, peripheral equipment and software, formed according to a subject or functional characteristic, designed to automate the reception processes, storing, processing and issuing information and focused on achieving ultra-high performance, or increasing the reliability, power, speed of computer technology in order to solve specific applied (highly specialized) tasks or a range of tasks on the information resources common for a given system”[21].
The prosecutor needs to pay attention to the fact that in this type of crime under a network of computers (computer network, information network, computer network) to understand:

1. The totality of the data transmission network, the electronic computers interconnected by it and the software and (or) technical means necessary for the implementation of this connection, which is intended for the organization of distributed information processing.

2. An interconnected set of geographically dispersed data processing systems, means and (or) telecommunication and data transmission systems, providing users with remote access to its resources and the collective use of these resources[22].

The subject of violation of the rules of informatization is an information system, a database, a data bank, a system for processing and transmitting information, and with authorized access to information systems without taking established protection measures - computer information protected by law, concentrated in a separate file, program, database as an object of intellectual property.

In this type of crime, the information system is an organizationally ordered set of information resources, information technologies and communication facilities, allowing the collection, storage, search, processing and use of information[23].

The database is in this form "a set of data (for example: articles, calculations), expressed in an objective form and systematized in such a way that this data can be found and processed using electronic computers"[24]. For example, reference databases for the population, databases of legislative and regulatory acts, databases of archival, museum, educational data.

In this type of crime, a data bank is an automated information system for centralized storage and collective use of data. The databank consists of one or more databases, a database reference book, a database management system, as well as a library of queries and applications[25]. Databanks of ministries, departments, research institutions, libraries, etc. can be cited as an example.

Under the system of processing and transmission of information, it is necessary to understand a system consisting of one or more computers, peripheral equipment and software that ensure the processing and transmission of computer information.

The creation of information systems, databases and data banks, systems for processing and transmitting information means writing software, selecting and installing hardware for the operation of an information system, databases and data banks, systems for processing and transmitting information for the purposes specified by the creator.

Implementation should be understood as the achievement of the practical use of information systems, databases and data banks, systems for processing and transmitting information according to their functional purpose.

The operation of information systems, databases and data banks, information processing and transmission systems should be understood as the process of their use.

Access to information systems is understood as the interaction of a person with electronic computers. Most often, such interaction is carried out for the purpose of further penetration to computer information, as a result of which a person is able to dispose of it at his own discretion (use, change, block, copy, destroy, etc.). Meanwhile, access to information systems (access to computers) should be distinguished from access to computer information. A person with access to the information system may not have access to the specific computer information stored in it.

It is impossible to recognize as access to information systems, as well as access to computer information, the seizure of electronic computers or machine information carrier as a thing, as well as the manipulation of computer information by external action on computer media of various kinds of radiation, mechanical impact, electromagnetic waves and other similar methods.

Authorized access to information systems is the interaction of a person with computer devices permitted (approved) by the owner or legal owner of the information system.
In turn, unauthorized interaction means that the user does not have the right to such actions, which indicates the illegal access.

Authorized access to information systems and the use of computer information is accompanied by strict observance of measures for its protection.

The presence of significant harm as a result of violation of the rules of informatization in each individual case is established by the investigating authorities and the court. This concept is of an evaluative nature, depends on the importance of the computer information itself and the determination of the amount of harm caused to the owner (owner) of the information system as a result of violation of the rules of informatization should be carried out taking into account the totality of all the data obtained. Significant harm in this situation can be recognized as the loss of important information, stoppage or interruptions in the work of an enterprise, organization, production activity, disruption of technological processes, causing moral harm to an individual by disclosing confidential information that constitutes personal, medical, legal secrets, etc.

The actions of a person, although related to a violation of the rules of informatization, but did not entail the consequences specified in the law, under certain circumstances can form an unfinished crime and qualify with reference to Art. 25 of the Criminal Code of the Republic of Uzbekistan.

The actions of the perpetrator are qualified under Part 2 of Art. 278 of the Criminal Code of the Republic of Uzbekistan if the violation of the rules of informatization entailed the infliction of especially large damage.

On the basis of the provisions of Section Eight of the Special Part of the Criminal Code of the Republic of Uzbekistan, "damage equal to three hundred or more minimum wages" is recognized as particularly large damage.

**Article 278. Illegal (unauthorized) access to computer information.**

According to the Criminal Code of the Republic of Uzbekistan, illegal (unauthorized) access to computer information is information in information and computing systems, networks and their components, if this action resulted in the destruction, blocking, modification, copying or interception of information, disruption of the operation of electronic computers, systems of electronic computers or their networks.

The direct object of illegal (unauthorized) access to computer information is public relations to ensure the security of computer information and the normal operation of computers, their systems or networks. Personal or property interests of citizens, or state or public interests can act as an optional object[26].

The subject of a crime can be any sane natural person who has reached the age of 16 by the time of the commission of the criminal act. It can be either a completely unauthorized person or a legitimate user who does not have the right to work with information of a certain category.

The objective side of the crime under Art. 278 of the Criminal Code of the Republic of Uzbekistan, is characterized by illegal (unauthorized) access to computer information, if these actions entailed the destruction, blocking, modification, copying, or interception of information, disruption of the operation of electronic computers, electronic computers or their networks.

On the subjective side, the crime under Art. 278 of the Criminal Code of the Republic of Uzbekistan, is committed with intent, direct or indirect. The perpetrator is aware of the fact of access to computer information without the permission of the owner (owner) of this information or in violation of the established access procedure, foresees and wishes or deliberately admits the occurrence of socially dangerous consequences specified in the law as a result of his actions. A careless form of guilt in this case may manifest itself when a person evaluates the legality of his access to information stored in a computer system, as well as in relation to the socially dangerous consequences that have occurred as a result.
The prosecutor, when checking the correct qualification of the corpus delicti by the bodies of inquiry and preliminary investigation, must pay attention to the fact that the subject of the crime, as directly indicated in the disposition of Part 1 of Art. 278 of the Criminal Code of the Republic of Uzbekistan is computer information, that is, information in information and computing systems, networks and their components.

Information in the constituent parts of an information-computing system or an information-computing network is information located in internal and external storage devices, computer memory, memory of peripheral devices and information passing through communication channels.

Access to computer information is any form of penetration to it, familiarization of a person with data contained in a network, system or on machine media.

One of the necessary grounds for bringing the guilty person to justice under the criminal law is the establishment of the illegality of his actions.

Illegal (unauthorized) access to computer information should be recognized as a person's acquaintance with data contained on computer media or in electronic computers without the right to such actions, that is, the permission of the owner (owner) of the information, or in the presence of such permission, but in violation of the rules of access control established in the system.

In other words, access to information is considered illegal if a person:

− does not have the right to access certain information;
− has such a right, but exercises it in violation of the established procedure.

The owner (owner) of computer information is obliged to establish the procedure for obtaining information by the user (indicating the place, time, responsible officials, necessary procedures, etc.) and provide conditions for users to access information.

Access control rules (ACR) are "a set of rules governing the access rights of subjects of access to access objects" [27].

“Any mechanism for controlling access to any information, regardless of whether it is about controlling the operation of processes or individuals, involves solving a number of problems:

− who has the right to access the system, information or resources in question;
− what specific elements of the resource this person can refer to;
− what the person can do with the object available to him;
− how the person is allowed to perform the necessary operations;
− under what circumstances can access be granted" [28].

According to Art. 11 of the Law of the Republic of Uzbekistan "On Informatization": Information resources according to the category of access are subdivided into public information resources and information resources with limited access.

Publicly available information resources are information resources intended for an unlimited number of users [29].

Information resources of limited access include information resources containing information about state secrets and confidential information or information, access to which is limited by the owners of information resources”.

The procedure for obtaining information from information resources is determined by the owner or owner of information resources in compliance with the requirements established by the law of the Republic of Uzbekistan "(Informatization". At the same time, a special mode of collection, storage, processing, distribution and use of information is established for information resources of limited access.

Information obtained legally from information resources by legal entities and individuals can be used by them to create derivative information with a mandatory link to the source of information.
The prosecutor, when checking the correct qualification of the corpus delicti by the bodies of inquiry and preliminary investigation, must pay attention to the fact that illegal (unauthorized) access to computer information always manifests itself in an active form of behavior of the perpetrator. It is impossible to commit this crime by inaction. At the same time, the methods of unauthorized access can be different (using someone else's password, changing the physical addresses of technical equipment, disguising as a legitimate user, finding weak points and "hacking" the system's protection, introducing into someone else's information system through "guessing the code", modifying software and information and so on), but they have no effect on qualifications.

The means of committing this crime is computer technology, that is, various types of electronic computers, hardware, peripheral devices, as well as communication lines, with the help of which computer technology is united into information networks.

It must be said that as a result of illegal (unauthorized) access to computer information, a person first of all gets the opportunity to get acquainted with this information, which is carried out, as a rule, by actually calling or viewing it. At the same time, the very fact of an illegal call or viewing of computer information stored on a machine carrier does not constitute a crime, but it can act as a preparation or attempt to commit another deliberate crime, for example, espionage (Article 160 of the Criminal Code), extortion (Article 165 CC), etc. In such cases, additional qualifications under Art. 278 of the Criminal Code of the Republic of Uzbekistan is not required.

The second mandatory sign of a crime under Art. 278 of the Criminal Code of the Republic of Uzbekistan, are socially dangerous consequences in the form of destruction, blocking, modification, copying or interception of information, as well as disruption of the operation of electronic computers, electronic computers or their networks, from the moment of occurrence, one of which is a crime finished. Moreover, between the onset of the consequences listed in the disposition of Part 1 of Art. 278 of the Criminal Code of the Republic of Uzbekistan, and the commission of illegal (unauthorized) access to computer information, a direct causal link must be established without fail.

Destruction of information is understood as complete or partial removal (erasure) of information from machine media, in which it ceases to exist due to the loss of the main qualitative features, cannot be restored and used for its intended purpose. At the same time, for the qualification of the deed according to the norm, it does not matter whether the victim had a copy of the information destroyed by the guilty person or not. In the same way, the unauthorized transfer of information to another electronic computer or to a machine medium should be regarded if, as a result of these actions, the information resource has left the possession of the owner or other legal user.

Blocking of information is a temporary or permanent impossibility of using it for its intended purpose (impossibility of performing any operations with computer information) by the owner (possessor) or a legal user, while the information itself is preserved. There is also such a concept as blocking the transmission of information (data), which is one of the violations in the field of information security and is expressed in the interruption of the transmission or delay of information for a time during which it will lose value for the user.

The prosecutor, when checking the correct qualification of the corpus delicts by the bodies of inquiry and preliminary investigation, must pay attention to the fact that the modification of information in this crime consists in an unauthorized change of the original content or volume of information (except for changes associated with the adaptation of the database) on its carriers during processing by technical. For example, deleting or adding records contained in database files, translating computer information from one language to another, reorganizing the database, etc.

Copying in the sense of the article means the transfer of the relevant information or part of the information from one physical medium to another while preserving the intactness of the original and the possibility of its further use for its intended purpose.
Interception of information should be understood as intentional misappropriation of information "not intended for public dissemination, committed by technical means directly from a computer system or from outside it, due to the removal of electromagnetic radiation that carries such information"[32].

Modern technical means make it possible to receive information without direct connection to a computer system: it is intercepted by radiation from the central processor, display, communication channels, printer, etc. All this can be done at a sufficient distance from the intercepted object. Interception methods can be different: direct (active) interception; forced interception; interception of characters; interception of messages; electromagnetic (passive) interception; audio interception (retrieval of information via vibroacoustic channels); video interception ("data pumping"), etc. Interception of information is carried out either directly through the external communication channels of the system, or by direct connection to the lines of peripheral devices. The objects of direct "eavesdropping" are cable and wire systems, terrestrial microwave systems, satellite communications systems, and special government communications systems[33].

Disruption of the operation of electronic computers, a system of electronic computers or their network consists in the occurrence of a non-standard situation with electronic computers or its devices, which creates temporary or permanent interference with their normal functioning (slowdown or incapacitation), provided that physical the integrity of electronic computers, systems of electronic computers or their networks. For example, malfunctions of information equipment, network breakdown, refusal to issue information, issue of distorted information, etc. If, along with the named failures, there is a violation of the integrity of computer equipment as a physical thing, the deed is qualified in conjunction with Art. 173 of the Criminal Code of the Republic of Uzbekistan.

It must be said that the alternative nature of those specified in the disposition of Part 1 of Art. 278 of the Criminal Code of the Republic of Uzbekistan, the consequences are due to the fact that the commission by a person of the same actions on illegal access to computer information often leads to different criminal results. As a rule, it depends on the protection of computer information, the degree of reliability of the computer system, the connection of the computer system with other systems, etc. A chain reaction is not excluded, when one criminal result provokes another.

It should be borne in mind that in the case when illegal (unauthorized) access to computer information acts as a method of committing another deliberate crime, and electronic computers are used as a tool for the implementation of criminal intent, the deed should be qualified according to the relevant article of the Criminal Code of the Republic of Uzbekistan. So, if the considered consequences were the result of another intentional influence on computer information that followed illegal access, then in the presence of the signs specified in the law, Art. 278⁴ or Art. 278⁵ of the Criminal Code of the Republic of Uzbekistan[34].

Unauthorized access to computer information without the intention to commit a socially dangerous act does not constitute a crime. For example, involuntary access to information due to an error of the direct user, etc.

The motives and goals of illegal (unauthorized) access to computer information are not mandatory signs of corpus delicts and, therefore, do not affect the qualification of a crime, but can be taken into account when assigning a just punishment to a guilty person[35].

Part 2 of Art. 278 of the Criminal Code of the Republic of Uzbekistan provides for circumstances that aggravate liability for illegal (unauthorized) access to computer information. These include the commission of a crime:

a) by prior conspiracy by a group of persons;
b) repeated or dangerous recidivist;
c) using the official position;
d) by an organized group or in its interests.

Clause "a" part 2 of Art. 278 of the Criminal Code of the Republic of Uzbekistan is incriminated in cases when persons who had previously agreed on its joint commission participated in a crime. For example, one member of a criminal group can open the security system, thereby providing direct access to computer information, and another - to perform appropriate manipulations with this information, leading to the occurrence of socially dangerous consequences specified in the law.

Under the use of official position in the sense of paragraph "c".

Art. 278 of the Criminal Code of the Republic of Uzbekistan should be understood as making access to computer information by a person who has the right to access by virtue of the work performed under a labor or civil law contract, or the impact by virtue of his official position on other persons who have such access.

When using his official position, a person actually uses the rights and obligations granted to him in the service, but violates the procedure for fulfilling these rights and obligations, i.e. goes beyond the limits of his powers in the service and gets the opportunity to dispose of computer information to which his rights and obligations do not extend or to which he does not have access.

The subjects of the crime under paragraph "c" of Part 2 of Art. 278 of the Criminal Code of the Republic of Uzbekistan, there can be both employees of organizations operating a computer system, and employees of a controlling organization. If the subject of the crime was an official, then, taking into account the circumstances of the case, it is possible to qualify for the totality of crimes under Art. 278 and Art. 205 or art. 206 of the Criminal Code[36].

Features of the qualification of illegal (unauthorized) access to computer information, committed repeatedly or by a dangerous recidivist, as well as by an organized group or in its interests, are identical to the similar qualifying features discussed by us above in relation to other offenses.

**Article 278. Manufacturing for the purpose of marketing, or marketing and distribution of special means for obtaining illegal (unauthorized) access to a computer system.**

According to the Criminal Code of the Republic of Uzbekistan, the manufacture for the purpose of marketing or the sale and distribution of special means for obtaining illegal (unauthorized) access to a computer system is the manufacture for the purpose of marketing or the sale and distribution of special software or hardware to obtain illegal (unauthorized) access to a protected computer system, as well as to telecommunication networks.

The direct object of this crime is public relations to ensure the safety of computer information and the normal operation of electronic computers, their systems or networks. Personal or property interests of citizens, or state or public interests can act as an optional object.

The subject of this crime is any sane natural person who has reached the age of 16.

The objective side of the crime under Art. 278 of the Criminal Code of the Republic of Uzbekistan, expressed in the manufacture for the purpose of marketing or marketing and distribution of special software or hardware to obtain illegal (unauthorized) access to a protected computer system.

On the subjective side, the crime under Art. 278 of the Criminal Code of the Republic of Uzbekistan, can be committed only with direct intent. The perpetrator realizes that he is making special means for obtaining illegal access to a computer system for the purpose of selling them, or he is aware that he is selling or distributing these means, and wants it. During production, it is also necessary to establish a specific purpose - the sale of the corresponding software or hardware.

The subject of the crime is special software or hardware for obtaining illegal (unauthorized) access to a protected computer system.

Software and hardware refers to computer hardware.
According to the state standard of Uzbekistan, a software tool in this corpus delicti is “an object consisting of programs, procedures, rules, as well as, if provided, accompanying documentation and data related to the functioning of the information processing system”[37].

The software includes:

- software - a set of control and processing programs, consisting of: system programs (operating systems, maintenance programs), application programs (programs that are designed to solve problems of a certain type, for example, text editors, antivirus programs, etc.) , as well as instrumental programs (programming systems consisting of programming languages: Turbo C, Microsoft Basic, etc. and translators of a complex of programs that provide automatic translation from algorithmic and symbolic languages into machine codes);
- machine information of the owner, owner, user.

According to A.A. Moskvitin. software is a program or a logical connected set of programs on machine storage media, supplying program documentation. In other words, software is the program itself and the documentation for it. This concept summarizes software tools[38].

Allaev S.S. believes that software is a set of programs that make the hardware part of the system perform the necessary actions, "animate" the computer. This part of the computer system is usually called "software".

In all concepts, there is no progress in the execution of certain algorithms that characterize software tools[39].

The prosecutor, when checking the correct qualification of the corpus delicti by the bodies of inquiry and preliminary investigation, must pay attention to the fact that the software in this type of crime is means (programs) designed for the automatic implementation of certain algorithms, which consist of individual commands and are processed sequentially, or the progress controlled by the program itself.

Software is an intelligent product regardless of the medium on which it is recorded.

Special software tools for obtaining illegal (unauthorized) access to a protected computer system are mainly programs designed to hack information protection from unauthorized access, copying, theft or modification of information.

Hardware is the hardware used to process data. This includes all mechanical, electrical and electronic equipment intended for automated data processing (personal computer, peripheral equipment and physical media of machine information).

Under special hardware in art. 278³ of the Criminal Code of the Republic of Uzbekistan means mechanical, electromechanical, electronic, optical, laser, radio, radio engineering, radar and other devices, systems and structures designed to break into the protection of a computer system from unauthorized access, copying, theft or modification of information stored.

In this structure, a protected computer system is a computer system capable of resisting illegal (unauthorized) access to information, the procedure for handling which is established by its owner (owner)[40].

Protection of a computer system is carried out primarily in order to protect the information contained in it.

The manufacture of special means for obtaining illegal (unauthorized) access to a computer system means that a person commits any actions aimed at creating these means. Thus, the manufacture of special software is expressed in the creation of computer programs intended for illegal access to a protected computer system. The manufacture of special hardware means the creation of various technical systems, instruments, devices for the same purpose, as well as alteration of standard devices, as a result of which they can be used for illegal access to a computer system.
The manufacture of special software or hardware for obtaining illegal (unauthorized) access to a protected computer system constitutes a crime only in cases where the perpetrator had the purpose of selling them.

Under the sales in art. 278³ of the Criminal Code of the Republic of Uzbekistan, prosecutors should understand any form of alienation of special hardware in favor of an indefinite circle of persons (in particular, by selling, donating, renting, lending, etc.), who are able to use them for their intended purpose.

In this case, distribution should be understood as the creation of conditions for access to special software, described in the disposition of the norm, to an indefinite circle of persons who, as a result, are able to use them. The methods of distributing software can be different (transmission by e-mail, by communication through a computer network, etc., as well as by sale, rental, renting, donation, etc.) and do not affect qualifications.

A crime is considered completed from the moment of manufacture (creation) of at least one copy of a special agent specified in the law, ready to be used for its intended purpose, or from the moment of sale or distribution of at least one of such agents.

Part 2 of Art. 278³ of the Criminal Code of the Republic of Uzbekistan provides for liability for the manufacture for the purpose of marketing or the sale and distribution of special means for obtaining illegal (unauthorized) access to a computer system, committed:

a) by prior conspiracy by a group of persons;
b) repeated or dangerous recidivist;
c) using the official position;
d) by an organized group or in its interests.

**Article 278⁴ Modification of computer information**

According to the Criminal Code of the Republic of Uzbekistan, modification of computer information is an illegal change, damage, erasure of information stored in a computer system, as well as the introduction of deliberately false information into it, causing major damage or significant harm to the rights or legally protected interests of citizens, or to state or public interests ...

The direct object of modification of computer information is public relations to ensure the safety of computer information and the normal operation of electronic computers, their systems, networks. An additional direct object is social relations that guarantee the realization of personal or property rights and interests of citizens, as well as state and public interests[41].

The objective side of the crime is illegal change, damage, erasure of information stored in a computer system, as well as the introduction of deliberately false information into it that has caused major damage or significant harm to the rights or legally protected interests of citizens, or state or public interests.

On the subjective side, the crime under Art. 278⁴ of the Criminal Code of the Republic of Uzbekistan, can be committed intentionally (with direct or indirect intent), through negligence or with a complex form of guilt.

The motive and purpose of the act are optional.

Akhramenka N.F. and Rustambaev M.Kh. consider that the modification of computer information is its processing, that is, the introduction of any changes that are not adaptation to the information stored in the computer system[42].

Yani P.S. believes that the modification of computer information, due to its partly blank nature, is understood both as a change in the software by means of which information is collected, stored, processed, transmitted, and as a change in the information array itself[43].

According to Panchenko P.N. by "information modification" is meant a change in the logical and physical organization of the database.
Kochoi S. and Savelyev D. believe that the modification can be carried out both by partial replacement of the original information with another, and by adding new information to the original[44].

According to N.A. Bochareva, modification consists in changing the initial state of information (for example, restructuring or reorganizing a database, deleting or adding records contained in its files, translating a computer program or database from one language to another), which does not change the essence of the object[45].

From the point of view of S.V. Borodin, modification of information means a change in its content compared to the information that was originally (before the commission of the act) at the disposal of the owner or legal user[46].

In investigative practice, the term "modification" of computer information is recognized as a concept that does not include such consequences as destruction, blocking, copying. As a result, it is recommended that when investigating crimes in the field of computer information, "modification" is understood to mean making changes to computer information (or its parameters)[47].

In our opinion, modification of electronic information means a change in the content of electronic information or software compared to the electronic information that was originally (before the commission of the act) at the disposal of the owner or legal user. Considering that for qualification under this article it does not matter what change and in what type of information (in the program or in the document) was made, the chief prosecutor, when checking the correct qualification of the corpus delicti by the bodies of inquiry and preliminary investigation, must establish that the information is protected by law and changes were made in it.

In any case, the issue of the legality of the modification made should be resolved taking into account the provisions of the Law of the Republic of Uzbekistan "On Copyright and Related Rights" dated July 20, 2006 [48].

By changing information, it is necessary to mean making various adjustments to the initial state of computer information (for example, restructuring or reorganizing a database, adding records contained in its files, translating a computer program or database from one language to another) that do not change its essence.

Damage to information should be considered making it unusable during processing by technical means, if there is a possibility of its recovery.

Erasing information stored in a computer system is actually its destruction and is an operation that makes a file or a fragment of it logically and physically inaccessible.

The introduction of deliberately false information in the sense of the norm consists in adding information that does not correspond to reality into the information stored in a computer system.

Illegal modification is considered to be a completed crime from the moment of occurrence specified in the disposition of Part 1 of Art. 278 of the Criminal Code of the Republic of Uzbekistan of socially dangerous consequences in the form of large damage or significant harm to the rights or legally protected interests of citizens, or state or public interests.

Significant harm as a result of the commission of this crime may consist in the loss of important or even especially valuable information; failure of important technical means (in particular, aircraft navigation equipment, which can lead to accidents, disasters and deaths); a break in communication between electronic computers, united in a computer network, requiring readjustment or long-term repair; etc.

As circumstances aggravating responsibility for illegal modification of computer information, Part 2 of Art. 278 of the Criminal Code of the Republic of Uzbekistan establishes the commission of a crime:

a) with causing especially large damage;
b) by prior conspiracy by a group of persons;
c) repeated or dangerous recidivist.

**Article 278. Computer sabotage**

Based on the wording of the disposition of the article, computer sabotage is the deliberate disabling of someone else's or service computer equipment, as well as the destruction of a computer system (computer sabotage).

The direct object of this crime is public relations to ensure the safety of computer information or programs, as well as computer equipment. Public relations that ensure the personal or property interests of citizens or state or public interests can act as an optional object here.

The objective side of computer sabotage is to disable someone else's or service computer equipment, as well as to destroy the computer system.

On the subjective side, this crime can only be committed with direct intent. The perpetrator realizes that he is taking actions aimed at disabling computer equipment or destroying a computer system and wants to commit them.

The subject of the crime is someone else's or company computer equipment, as well as a computer system.

According to the explanatory dictionary of S.I. Ozhegova, sabotage means "malicious, deliberate disorder or disruption of work, while observing the appearance of its fulfillment, latent opposition to the fulfillment, the implementation of something"[49].

According to Stepanov O.A. computer sabotage is the entry, alteration, erasure or suppression of electronic data or computer programs, or the entry into computer systems for the purpose of making the computer or telecommunication systems operational[50].

Susloparov A.V. believes that computer (logical) sabotage is deliberate unlawful damage, deletion or alteration of data that has caused significant harm or has caused the creation of obstacles to the operation of a computer system[51].

According to Y. Beketnov, S. Krylov, S. Larionov, computer sabotage is the erasure, damage, deterioration or suppression of computer data or programs without the right[52].

The prosecutor, when checking the correct qualification of the corpus delicti by the bodies of inquiry and preliminary investigation, must pay attention to the fact that computer sabotage is the deliberate withdrawal of computer equipment, as well as the destruction of computer systems if this action entailed the erasure, damage, deterioration or suppression of computer data or programs without the right for that.

In this type of crime, computer equipment is equipment designed to transform and store information. This type of equipment includes equipment for communication systems and means, measurement and control means, computer technology (analog and analog-digital machines for automatic data processing, electronic computing, electromechanical and mechanical complexes and machines, devices designed to automate storage processes, search and data processing associated with solving various problems) and office equipment, visual and acoustic display of information, information storage media, theater and stage equipment, etc[53].

Disabling computer equipment means making certain elements of a computer system, network, electronic computers unusable, which significantly complicates their functioning in accordance with their intended purpose.

The destruction of a computer system should be understood as the destruction of both all hardware (technical) components of the system, and some of them, as a result of which this system ceases to function. Moreover, additional qualifications under Art. 173 of the Criminal Code of the Republic of Uzbekistan is not required.
The method of committing computer sabotage can be physical (destruction of blocks, disabling floppy disks, magnetic drums, disks, tapes, etc.) or hardware and software (Replacing devices with incompatible devices with a given computer, its system or network; recording over the database of game programs; changing the names of files, etc.), however, this does not affect the legal assessment of the actions of the culprit.

Computer sabotage is recognized as a completed crime from the moment a person commits the actions specified in the disposition of the article, i.e. from the moment someone else's or service computer equipment is disabled or a computer system is destroyed.

Part 2 of Art. 278\(^5\) of the Criminal Code of the Republic of Uzbekistan provides for increased liability for computer sabotage committed:

a) by prior conspiracy by a group of persons;
b) repeated or dangerous recidivist.

**Article 278\(^6\). Creation, use or distribution of malicious programs**

According to the Criminal Code of the Republic of Uzbekistan, creating computer programs or making changes to existing programs for the purpose of unauthorized destruction, blocking, modification, copying or interception of information stored or transmitted in a computer system, as well as the development of special virus programs, their deliberate use or distribution.

The direct object of this crime is public relations to ensure the safety of computer information and the normal operation of computers, their systems or networks. Personal or property interests of citizens, or state or public interests can also act as an optional object.

The subject is a sane natural person who has reached the age of 16. Typically, this is a person with specialized knowledge of cybernetics and information technology.

The objective side of the crime under Art. 278\(^6\) of the Criminal Code of the Republic of Uzbekistan, expressed in the creation of computer programs or changes in existing programs for the purpose of unauthorized destruction, blocking, modification, copying or interception of information stored or transmitted in a computer system, as well as the development of special virus programs, their deliberate use or distribution ...

On the subjective side, this crime can only be committed with direct intent. A person knowingly knows about the harmful properties of the program he creates, deliberately makes such changes to existing programs, develops special virus programs, uses or distributes them, and desires it. These actions are committed by the guilty person with the disposition of Art. 278\(^6\) of the Criminal Code of the Republic of Uzbekistan for the purpose of unauthorized destruction, blocking, modification, copying or interception of information stored or transmitted in a computer system. The motive for the offense is optional.

The subject of the crime is formed by malicious computer programs, as well as special virus programs, that is, programs that can infect other programs.

A computer program (program for electronic machine) is "a set of data and commands expressed in an objective form and intended for the operation of computers, computer networks and other computer facilities in order to obtain a certain result"[54]. The preparatory material obtained during its development and the audiovisual displays generated by it are also recognized as a computer program.

It is important to emphasize that the disposition of Art. 278\(^6\) of the Criminal Code of the Republic of Uzbekistan deals specifically with a malicious computer program (computer program). According to Rustambaev M.Kh. malicious computer programs in this type of crime are specially created programs capable of performing unauthorized actions by the user and thereby causing harm to the owner (owner) of information stored or transmitted in a computer system in the form of its
destruction, blocking, modification, copying or interception, and also the onset of other adverse consequences (disruption of the operation of a computer, computer system or their network).

Malykottsev M. M. believes that “a malicious program is a program specially written in any programming language, the use and distribution of which in an information system or in an information and telecommunication network leads to illegal influence on information and (or) on computer equipment and communications , expressed in illegal destruction, copying, damage, blocking, distortion of information, and (or) other violation of the order of operation of these devices established by the legal owner” [55].

E. A. Maslakova determines the harmfulness of a computer program in a similar way, noting that its essential property is the ability to cause destruction, blocking, modification or copying of computer information unauthorized by the owner[56].

In turn, Efremova M.A. emphasizes that the main difference between malicious programs and others, which can also copy, destroy, modify information, is determined by the fact that all actions are performed without notifying the user, secretly from him, and the user himself often unaware of the presence of such a program on his computer[57].

To determine the maliciousness of a program, it is necessary to find out whether it is capable of leading to unauthorized blocking, copying, modification, destruction of data or programs stored in computer systems, i.e. whether it is intended to inform the owner (owner) or another competent user of information about the nature of this action. program, as well as whether it is expected to obtain his permission for the program to implement its functions. If at least one of these requirements is violated, the program should be declared illegal (malicious).

Kuznetsov A.P. also substantiates that the harmfulness or usefulness of the corresponding computer programs is determined not depending on their purpose, the ability to destroy, block, modify, copy information (this may be a technical function of licensed (permitted) computer programs), but that assumes whether their action is, firstly, prior notification of the owner of computer information or another conscientious user about the nature of the program's operation, and secondly, obtaining his consent (authorization) for the program to implement its purpose. Violation of one of these requirements makes the computer program malicious[58].

According to Vekhov V.B., in order to recognize a computer program as malicious, it is necessary to prove the presence of a combination of the following circumstances:

1) the program is capable of destroying, blocking, modifying or copying computer information or neutralizing the means of protecting computer information;

2) the program does not provide for prior notification of the owner, owner or user (possessor) of computer information, computer device, information system or information and telecommunications network about the nature of its actions;

3) the program does not ask for consent (sanction) from the owner, owner or user (possessor) of computer information, computer device, information system or information and telecommunications network to implement its purpose (algorithm)[59].

In the light of the modern threats of a rapidly "virtualizing" society, we believe that the only correct choice is to choose its original and main purpose as the main criterion for the maliciousness of a program - the implementation of illegal activities.

The prosecutor, when checking the correct qualification of the corpus delicti by the bodies of inquiry and preliminary investigation, must pay attention to the fact that a malicious program should be understood as a computer program created (including by modifying a legal program) to carry out illegal activities.

Such an interpretation, in our opinion, will make it possible to prevent in the future possible problems in the use of such an operational-search measure as obtaining computer information.
The category of malicious programs includes: virus programs; software-emulators of electronic keys; password cracking programs; "Logic bombs"; programs like "Trojan horse", "worms", etc.

One of the most widespread among all malicious programs at one time (2001) was a Trojan horse program designed to intercept computer information and establish control over someone else's electronic computer. This program represents blocks of commands not provided by the software developer, self-destructing at the end of its task. After that, finding these program modules is almost impossible[60]. The peculiarity of Trojans is that they penetrate deeply into the computer system, are carefully masked, and therefore it is very difficult to detect and remove them.

No less popular are "logic bombs", which are "deliberate changes in the program code, partially or completely disabling the program or the electronic computing system under predetermined conditions, for example, the onset of a certain time[61].

The fundamental difference between "logic bombs" and computer viruses is that they are initially part of a program and do not pass into other programs, and computer viruses are dynamic programs and can spread even over computer networks."

A virus program is a special malicious program that can spontaneously attach itself to other programs (that is, "infect" them) and, when the latter are launched, perform various actions that are undesirable for a competent user: damage to files and directories, leading to destruction, modification, blocking information; clogging or erasure of the computer's memory, resulting in a slowdown in its work, etc[62].

Virus programs usually include commands for self-copying and masking. For a certain period of time, the virus may not detect itself, but then the computer "gets sick" and outwardly breaks down for no reason. Most often, computer malfunctions are accompanied by complete or partial destruction of information.

Among the most well-known officially registered computer viruses that can make a computer completely unusable, one can name "Pakistani virus", "Christmas tree", "Morris virus", "I love you", "666". At present, the number of viruses for electronic computers reaches several thousand and their number is constantly growing.

Distribution of a malicious or special virus program means the provision of access to a malicious program reproduced in any material form, including by network and other means, as well as by selling, renting, renting, lending, including importing for any of these purposes[63]. The distribution of the considered type of programs can be carried out directly by copying them to the victim's computer, for example, from a floppy disk or other medium, as well as indirectly, by transmission through the communication line of a legitimate user through a computer network or by e-mail.

The crime under Art. 278 of the Criminal Code of the Republic of Uzbekistan, is recognized as completed from the moment of committing any of the actions provided for in the disposition of this norm, regardless of the onset of consequences in the form of destruction, blocking, modification, copying or interception of information stored or transmitted in a computer system. Thus, the presence of the source code of virus programs is already the basis for prosecution under the article.

It should also be clarified that "an act expressed in the creation of malicious programs or changes in existing programs constitutes a crime only when such an act objectively created a real threat of unauthorized destruction, blocking, modification or copying of information. Otherwise, the person's actions to create, the use or distribution of malware should not be considered a crime. For example, the actions of a person who has created a rather harmless virus program that displays a stroke on the monitor screen and disappears immediately will not be criminal [64].

Therefore, in cases where the created, distributed or used malicious program objectively cannot lead to blocking, modification, copying or interception of information, without thereby posing a danger
to its owner, the actions of the perpetrator should be regarded as insignificant on the basis of Art. 36 of
the Criminal Code.

Part 2 of Art. 278 of the Criminal Code of the Republic of Uzbekistan regulates the commission
of a crime:

a) with causing especially large damage;
b) by prior conspiracy by a group of persons;
c) repeated or dangerous recidivist;
d) by an organized group or in its interests.

Article. 278ב Illegal (unauthorized) access to the telecommunications network.

According to the Criminal Code of the Republic of Uzbekistan, Illegal (unauthorized) access to
a telecommunications network is illegal (unauthorized) access to a telecommunications network for
the purpose of using it and passing international traffic bypassing installed security systems, as well as
storing and creating conditions for the functioning of special software or hardware.

To date, the qualification of this crime has not been fully studied by modern scientists and the
question of the composition of the crimes remains open. When investigating crimes, the investigator
must correctly qualify the crimes, the wrong qualification of the crime will lead to the prosecution of
an innocent person or substitute a less serious crime for a serious crime.

Conclusion

Having studied more than 50 criminal cases, we came to the conclusion that illegal
(unauthorized) transmission of international traffic bypassing the installed protection systems means
the substitution of international traffic of a certain cellular company for a local one, by redirecting a
VoIP call from abroad to a local GSM network (gateway). The call is charged as local, and you can
earn money on the difference in cost.

Here, hardware means special communication equipment.

Consequently, the direct object of this crime is public relations to ensure the safety of computer
information and the normal operation of electronic computers, their systems or in the network.

The objective side of this crime is illegal (unauthorized) access to the telecommunications
network

The subject of this crime is a person who organizes illegal connection to telecommunication
networks and the transmission of international traffic.

On the subjective side, the crime provided for in this article of the Criminal Code of the
Republic of Uzbekistan can be committed only with direct intent. The perpetrator realizes that he has
illegally (unauthorized) gained access to the telecommunications network.
REFERENCES


43. Yani P. Special types of fraud // Legality. 2015. No. 8; SPS "Consultant-Plus" P. 25-34.
47. Methodological recommendations for the implementation of procuratorial supervision over the implementation of laws in the investigation of crimes in the field of computer information (approved by the Prosecutor General's Office of Russia). URL: http://lawru.info/dok/2013/01/07/n14846.htm. Date of access: 08.06.2020.