CRIME PREVENTION IN THE FIELD OF COMPUTER TECHNOLOGIES AT THE PRESENT STAGE IN THE RUSSIAN FEDERATION: PROBLEMS AND WAYS TO SOLVE THEM

INTRODUCTION

In the XXI century, digital information has acquired a special social, economic and legal value. The famous phrase of Rothschild “who owns information—he owns the world”, today looks quite reasonable. Indeed, at present, the material well-being of many people is based on information stored in electronic form, state security systems have been developed on it, and breakthroughs in modern science are unthinkable without it. Access codes to missiles and bank cards, various databases (for example, taxpayers), electronic document management systems and management of medical equipment, gas, water, energy supply, etc. The list can be continued indefinitely (PETROVA, LOBACHEV, 2020).

Computer information plays an essential role in all spheres of life of modern society. Accordingly, the protection of private, public and state interests in the field of computer information is an urgent problem. It should be emphasized that modern IT technologies penetrating into all spheres of human life lead to the emergence and development of not only positive trends, but also negative ones. Crime also uses scientific and technological achievements for its own purposes. The most striking example is computer crimes, which are becoming not only stable, but also acquire an economically oriented, organized character.

The scale of the damage caused by computer crimes is impressive. Over the past three years, the dynamics of the increase in crimes in the field of IT technologies in Russia amounted to 165%. In 2017, 66 thousand such crimes were committed, in 2018 – 175 thousand, and in 9 months of 2019 – more than 200 thousand. In 2019, every 7 crimes in the Russian Federation were committed with the help of IT technologies. The total amount of material damage caused is more than 10 billion rubles (FALALEEV, 2019). The damage caused by cybercrime in Russia amounted to 69 billion rubles in 2020 (GUNKEL, 2021).

Thus, the development and implementation of criminal law measures aimed at combating and preventing cybercrime in Russia is the most important area of activity to ensure a high level of information security of the Russian society. It should be noted that the current criminal legislation of the Russian Federation does not contain a sufficiently developed regulatory framework for the implementation of responsibility for the crimes of the group in question, taking into account their real danger to society. Some of the acts that have a sign of public danger have not yet been criminalized in criminal legislation (Criminal Code of the Russian Federation No. 63-FZ of 13.06.1996 (ed. of 01.07.2021), (https://base.garant.ru/77683496/). The current domestic criminal legislation does not provide for the normative consolidation of such concepts as “the use of computer technologies”, “computer technologies”, “crimes committed using computer technologies”, etc.

The above factors have a direct impact on preventive and law enforcement activities, reducing their quality. It is the imperfection of the existing legal system that allows offenders to evade responsibility, significantly complicating their criminal prosecution. This creates conditions for the commission of new crimes. These circumstances, which indicate the undoubted relevance of the criminal-legal aspect of countering crimes in the field of using modern computer technologies, determine the relevance, theoretical and practical significance of this study.

AUTHORSHIP

Dina Viktorovna Alontseva

D. yurid.N., Associate Professor, Associate Professor of the Department of Jurisprudence Federal State Budgetary Educational Institution of Higher Education «Bunin Yelets State University».

ORCID: https://orcid.org/0000-0003-2486-9248
E-mail: dina.alontseva@mail.ru

Olga Anatolyevna Lavrishcheva

K. yurid.N., Associate Professor, Associate Professor of the Department of Jurisprudence Federal State Budgetary Educational Institution of Higher Education «Bunin Yelets State University».

ORCID: https://orcid.org/0000-0003-4012-5505
E-mail: lavrishcheva-olga@mail.ru

Received in: 2021-07-02
Approved in: 2021-08-02
DOI: https://doi.org/10.24115/52486-62020217Extra-E1222p.445-460
LITERATURE REVIEW
The problem of the legislative definition of computer information at the present stage of the development of information technologies, as well as the issues of defining the concept of the object of criminal legal protection and the subject of criminal encroachments in the field of computer (digital) information are analyzed in the works of: Petrova, Lobacheva (2020); Rassolova (2008), etc.

The analysis of modern scientific approaches to the definition of the concept, structure and essence of computer crime in Russia is carried out in detail in the periodic publications of domestic researchers: Gunkel (2020); Ev dokimov (2016); Kochkina (2017). The most complete issues of criminal and legal assessment of computer crimes are covered in the works of such Russian specialists as Nomokonov, Tropina (2013); Dorovskikh (2016); Komarov (2017); Chirkov, Sarkisyan (2013); Mal ykovtsev (2006).

Modern scientific approaches to the prevention of computer crime in the Russian Federation and the development of an effective set of preventive measures to counteract computer crimes are covered in the works of: Emirov, Saidova, Ragimkanova (2011); Parkhomenko, Ev dokimova (2015); Temiraliev, Omarova (2019); Anosova (2018).

Thus, it can be observed that a large number of concepts, ideas and scientific views have accumulated in the arsenal of Russian science, devoted to general issues of legal characteristics of crimes in the field of computer (digital) information. At the same time, the analysis of domestic scientific works on the topic under study shows that in the science of Russian law insufficient attention is paid to the criminal-legal aspect of countering crimes in the field of using modern computer technologies, and a set of interrelated and complementary special organizational-legal, managerial and forensic measures that are aimed at preventing and preventing computer crimes in the Russian Federation has not been formed.

By their very nature, crimes in the field of computer information are cross-border, and therefore all international organizations call on States, in cooperation with other interested parties, to develop the necessary legislation providing for joint investigations of these acts using existing international law. In this regard, we can distinguish a number of foreign scientists whose works cover in detail the general issues of cybercrime: Jahankhani, Al-Nemrat, Hosseini-Far. (2015); Ali Al-Garadi, Varatan, Ravana (2016); Sammons, Cross (2017); Kimberly, Detardo-Bora, Dhruva, Bora (2016); Yerzhanov, etc. (2017) and others.

METHODOLOGY
When writing the work, the authors used the provisions of the dialectical method of cognition of social phenomena, as well as the techniques of formal logic and such general scientific methods as analysis, synthesis, analogy, comparison, induction, deduction, system analysis. In addition, private scientific methods were used: the method of systematic, comparative analysis and other methods. The system method made it possible to identify existing approaches to the state and structure of computer crime in the Russian Federation, certain patterns of causes and conditions for committing crimes in the field of high computer technologies. The method of content analysis made it possible to ensure the completeness, reliability and consistency of the data obtained as a result of generalization.

The comparative legal method is based on an appeal to the theoretical and practical experience of law enforcement organizations, judicial bodies, on a comparison of Russian legal institutions and, as a result, a deeper understanding of the concept and essence of computer crime, identifying shortcomings in the criminal legislation of the Russian Federation. With the help of prognostic methods, the trends in the development of the object under study were determined and a vision of possible positive or negative consequences of the implementation of the provisions of Russian legislation in this area was provided.

The legal analysis was based on an assessment of the wording of the current Russian legislation from the standpoint of their effectiveness in combating certain groups of crimes in the area under consideration.

In order to develop a set of special legal, ideological, managerial, organizational and criminalistic measures aimed at the prevention and prevention of computer crimes, the authors
actively used statistical data obtained in the GIAC of the Ministry of Internal Affairs of Russia; quantitative indicators presented by independent centers for the study of cybercrime; materials of judicial practice of courts of general jurisdiction of the Russian Federation in criminal cases on crimes committed using computer technologies, reflecting the most pressing problems of practical law enforcement.

The use of the above methods in their totality made it possible to conduct a comprehensive and comprehensive study of the problems of crime prevention in the field of computer technologies at the present stage in the Russian Federation, as well as to substantiate the conclusions obtained.

RESULTS
At the present stage, the most urgent problem of the development of Russian society and the state is computer crime, which causes huge damage to information, cultural, scientific and technical, economic, social and political relations.

In 2016, Kaspersky Lab conducted an analysis of the damage caused by the activities of cybercriminals on the domestic market. According to the report, with a successful hacker attack, large corporations lose up to 20 million rubles, and small and medium-sized enterprises about 780 thousand rubles (lost profit, forced downtime, additional costs for paying for the services of specialists). Large enterprises additionally spend up to 2.1 million rubles on preventive measures and elimination of negative consequences, and medium-sized and small businesses up to 300 thousand rubles (EVDOKIMOV, 2016).

In this regard, the need to protect citizens and organizations from unauthorized access to computer data, from cyber espionage, from virus programs and other computer threats is becoming increasingly urgent. The current Criminal Code of the Russian Federation does not fix the concept of "computer crimes". This concept is included in the criminological group. Computer crime (cybercrime) is a set of crimes, in which computer data acts as the subject of criminal encroachment.

Computer crime is a complex criminal phenomenon that is considered in a broad and narrow sense. In a narrow sense, computer crime is a set of crimes in which information and telecommunications networks; computer devices; computer data; means of creating, transmitting, processing, protecting and storing computer data act as an instrument and object of crime. So, the concept of "computer crimes" coincides with the concept of "crimes in the field of computer data", established by law.

In a broad sense, computer crime is a set of crimes committed by sane individuals who infringe on the legitimate interests and rights of citizens, organizations, society and the state in the field of safe circulation, creation, protection, receipt, transmission, processing and storage of computer data, as well as the functioning of information and telecommunications networks, computer devices and other means of creating, distributing and using computer data.

In our opinion, the term "computer crime" in its broad sense is much larger in its content and scope than such concepts as "Internet crime", "cybercrime", "crime in the field of computer data", "crime in the field of IT technologies". It includes the above concepts as signs of the objective side of the corpus delicti (instrument, means, method of crime). This approach to the understanding of computer crime makes it possible to assess the diversity, complexity and multidimensional nature of the criminal phenomenon under study. This will allow us to find a balance among the existing scientific and theoretical positions.

Modern legal scientists often use the concept of "cybercrime", which means "crimes in the field of high computer technologies", "information crimes", "crimes in the field of computer data", "crimes in the information space", "crimes related to technical computer means", etc. Attempts to give a theoretical interpretation of the concept under consideration have been made by many researchers and scientists. For example, Tropina T. L. and Nomokonova V. A. believe that cybercrime is a broader category than "computer crime". It more accurately and fully reflects information crime (NOMOKONOV, TROPINA, 2013).
In our opinion, the most complete definition that reflects all aspects of the phenomenon under consideration is formulated by D. N. Karpov. The researcher believes that cybercrime should be understood as an act of social deviation in order to cause damage (cultural, ideological, moral, political, economic and other) to the state, society or a specific person using any technical device with access to the Internet (KOCHKINA, 2017).

Dorovskikh L. A. suggests that cybercrimes should be classified as crimes in the field of high technologies. According to the author, cybercrime is an act of social deviation in order to cause damage of any kind to the state, organizations or citizens using any technical device or means with access to the global network (DOROVSKIKH, 2016).

Komarov A. A. does not give clear boundaries to the concepts under consideration. He suggests that two groups of crimes should be included in the number of crimes in the field of high technologies: computer crimes; crimes committed with the help of IT technologies and the Internet (KOMAROV, 2017).

We adhere to the point of view of I. M. Rassolov, who in his dissertation research "Law and the Internet: theoretical problems" suggests using the term "crimes in the field of high technologies" for "the sphere of combating cybercrime (fraud on the Internet, interception of valuable information, hacking networks, dissemination in the virtual space of slanderous information about citizens, pornographic products, computer viruses, etc. D.)", equating cybercrime with a computer crime, highlighting its main feature in the use of computer networks to commit an illegal act or crime in virtual space (RASSOLOV, 2008). Thus, the concept of "cybercrime" is used as a synonym for the concept of "computer crime".

In our opinion, the analysis of the structure of computer crime (cybercrime) should be carried out precisely on the basis of the broad meaning of this concept, as well as taking into account existing doctrinal, expert and regulatory approaches.

Analyzing the normative approach to the structure of cybercrime reflected in the Information Security Doctrine of the Russian Federation [Decree of the President of the Russian Federation of 5.12.2016 No. 646 “On approval of the Information Security Doctrine of the Russian Federation” (https://www.garant.ru/products/ipo/prime/doc/71456224/)], we will highlight a number of illegal acts that act as the most serious threats to the security of information and telecommunications systems and means:

- unauthorized data collection and use;
- violation of data processing technology;
- introduction of elements into software and hardware products that implement functions that are not provided for in the documentation for these products;
- development and distribution of programs that disrupt the full functioning of ICT, including data protection systems;
- damage, destruction, electronic destruction or suppression of data processing systems and facilities;
- damage, destruction, theft or destruction of machine and other information carriers;
- unauthorized access to data stored in databases and data banks.

The Convention on Crime in the Field of Computer Information ETS No. 185 of 23.11.2001, signed in Budapest in 2001, established 5 groups of cybercrimes that form computer crime:

- crimes against the availability, integrity and confidentiality of computer systems and data;
- offenses involving the use of computer tools;
- offenses related to the content of computer information;
- offenses involving violation of copyright and related rights;
• Acts of xenophobia and racism committed with the help of computer systems and networks [Convention on Crime in the Field of Computer Information ETS of 23.11.2001 No. 185. (https://base.garant.ru/4089723/)].

This Convention has been ratified by 50 countries. Russia has not yet joined this international document. Despite this, the Russian practice has adopted the above classification.

It should be noted that the Russian legislator in the dispositions of Articles 171.2, 242, 242.1 and 242.2 of the Criminal Code of the Russian Federation provided for a special qualifying feature, which reads as follows: acts committed using the media, including telecommunications and information networks (including the Internet). A more severe punishment is provided for the commission of these criminal acts. According to the considered feature, the act provided for in paragraph “b” of part 2 of Article 228.1 of the Criminal Code of the Russian Federation should belong to computer crimes.

Despite the established regulatory approach of Russian law enforcement agencies to the structure of cybercrime, experts and specialists in the field of information security have their own opinion about the structure of computer crime in the Russian Federation.

Experts of the international organization "Group-IB", specializing in the investigation and prevention of computer crimes, identify the following main criminal acts that form the cybercrime market in the Russian Federation: sale of downloads, traffic and exploits; fraud in the Internet banking system; theft of electronic money; phishing; spam; services for cashing out illegal income; anonymization; DDoS attacks.

Specialists of the Kaspersky Lab Center for Global Research and Threat Analysis (GReAT) analyze the state of computer crime in the Russian Federation and other countries on an annual basis. Among the computer crimes, experts include:

• creation and use of botnets;
• cyber extortion;
• using exploits for software vulnerabilities;
• violation of privacy;
• targeted phishing;
• use of malware;
• cyber mercenary (cyber attacks committed for hire);
• theft of confidential information;
• hacktivism;
• cyber espionage;
• targeted cyber attacks.

Experts of the Panda Labs laboratory, which is part of the international company" Panda", engaged in the production of antivirus programs, named a number of crimes that in 2019 formed computer crime in the Russian Federation:

1. Hacking of devices connected to the Internet.
2. ART attacks - targeted attacks aimed at strategically important institutions and large companies.
3. Cyber attacks on payment terminals in order to steal customer bank card data.
4. Targeted cyber attacks on the information resources of institutions, enterprises, organizations, companies.
5. Cyber blackmail.
6. Attacks on smartphones and other mobile devices in order to steal data and passwords.

The opinion of experts on computer crimes and the structure of computer crime does not coincide with the normative approach that law enforcement agencies adhere to, since it is based on technical and program criteria. But the opinion of the expert community does not contradict the approach of law enforcement officers, since most cyber threats fall under the Criminal Code of the Russian Federation (for example, under the articles 146, 159.3, 159.6, 163, 165, 272-274 THE Criminal Code of the Russian Federation).

The analysis of the scientific literature on the topic confirms the lack of uniformity of opinions in science about the structure of computer crime. For example, Sargsyan A. J. and D. K. Chirkov distinguish the structure of computer crime only those crimes which the MIAC of the MIA of Russia considers as crimes committed in the field of computer data and telecommunications (CHIRKOV, SARGSYAN, 2013).

Ragimkhanov D. A., Saidov A. D. and Emirs M. B. believe that the most common types of crime on the Internet include:

- fraud;
- password hacking (spoofing);
- vandalism;
- sabotage;
- industrial espionage (EMIROV, SAIDOV, RAHIMKHANOV, 2011).

Other researchers believe that the structure of computer crime is more complex, and consider the crimes included in it according to a number of criteria:

- by the method of commission;
- on the subject of criminal encroachment;
- according to the object of the crime (crimes against confidentiality, availability and integrity of computer networks and data; computer crimes against state and public interests; computer economic crimes, etc.) (NOMOKONOV, TROPINA, 2013).

The largest share is occupied by such computer crimes:

- crimes in the field of computer information (articles 272-273 of the Criminal Code of the Russian Federation);
- fraud in the field of computer data (Article 159.6 of the Criminal Code of the Russian Federation).

Having analyzed the existing approaches to the state and structure of computer crime in the Russian Federation, we formulated the concept of "computer crime" in a broad and narrow sense. Based on the conducted research, the following key features of computer crimes can be identified:

- non-standard ways of committing;
- cross-border nature;
- automation of crimes;
- high incomes from crimes;
- interaction of different criminal communities;
- difficulty of disclosure;
- anonymity.
The structure of computer crime in Russia includes not only crimes in the field of computer data, but also a significant number of crimes committed with the help of information and telecommunications networks. We emphasize that the number of crimes provided for in Articles 272-273 and 159.6 of the Criminal Code of the Russian Federation (illegal access to computer data, creation, distribution and use of virus programs, fraud in the field of computer data) will increase in the near future. There are objective reasons for this, such as:

- informatization of society;
- development of IT technologies;
- imperfection of the current criminal legislation;
- errors and shortcomings of investigative and judicial practice in cases of the category under consideration;
- lack of the necessary number of qualified specialists in the law enforcement agencies to solve crimes of the category under consideration.

**DISCUSSION**

The emergence and rapid development of computer crime is one of the social problems of modern society. It causes serious harm to all spheres of the state - information, educational, scientific, cultural, political, economic, etc. The issue of protecting people, state and municipal institutions, authorities and enterprises from unauthorized access to computer data, from virus programs, as well as from all kinds of computer threats is becoming particularly relevant.

The scale of the damage caused by cybercrime is simply impressive. The dynamics of the increase in computer crimes in the field of IT technologies has increased significantly in Russia over the past three years. For example, according to Sberbank of the Russian Federation, the damage to our country’s economy from cyber threats in 2020 amounted to almost 3.5-3.6 trillion rubles. These are losses for both companies and citizens. Most of all, private businesses and the population suffer from cybercrime: state structures are attacked less, since the FSB immediately joins the investigation, which has its own monitoring, analytics and standards. According to the calculations of the state bank, there are now about 2.3 million Russian-language accounts in the darknet that operate with stolen data and organize criminal groups. The main jurisdictions for Russian-speaking cybercriminals are Russia, Ukraine, and Germany (VORONOVA, 2020).

Therefore, at present, the activities on the development and implementation of effective criminal legal measures to prevent and combat cybercrime are of particular relevance. The most important step in this direction was taken by Vladimir Putin, who signed a decree in 2016 approving the "Doctrine on Information Security of the Russian Federation". This document defines a number of fundamental goals: identification, neutralization, weakening, elimination of criminogenic factors that affect the growth of computer crime.

General preventive measures to prevent computer crime are universal in nature. They are focused on the prevention of crime in all areas, including computer crime. In our opinion, they were quite succinctly and clearly reflected in the Decree of the President of the Russian Federation No. 537 of 12.05.2009 [Decree of the President of the Russian Federation of 12.05.2009 No. 537 "On the National Security Strategy of the Russian Federation until 2020". (https://www.garant.ru/products/ipo/prime/doc/95521/). For example, among the general political measures to prevent computer crime in Russia are: ensuring the constitutional system; developing civil society and democracy; maintaining the sovereignty and territorial integrity of the Russian Federation. General economic measures of a preventive nature include:

- measures to ensure economic growth;
- measures to improve the competitiveness of the national economy;
- measures for the development of the innovation system of the Russian Federation;
measures to increase investment in human capital;
measures to increase labor productivity.

General social measures include:
- measures to reduce the level of property and social inequality;
- measures to stabilize the population in the medium term (and in the long term - to radically improve the socio-demographic situation);
- measures to ensure personal safety;
- measures to increase the availability of comfortable housing, provide the population with safe and high-quality goods and services, etc.

Scientific and technical general preventive measures include:
- measures to create a system of targeted applied and fundamental research;
- measures for state support in the interests of scientific and organizational support for achieving strategically important national priorities;
- measures to create a network of national research institutes and federal universities that provide training of qualified specialists for work in the educational and scientific field;
- measures to develop competitive technologies;
- measures for the organization of high-tech production.

General spiritual and cultural preventive measures include the following:
- measures to recognize the primary role of culture for the revival of cultural and moral values and their preservation;
- measures to strengthen the spiritual unity of the multinational people of the Russian Federation;
- measures to maintain the international image of Russia;
- measures to create a system of patriotic and spiritual education of Russian citizens.

Within the framework of this study, it is advisable to address the issue related to special measures to prevent cybercrime. The most important measure is the improvement of the current domestic criminal legislation. In our opinion, it is advisable to fix at the legislative level some legal concepts contained in the dispositions of Articles 272-274 of the Criminal Code, namely:

- computer program (computer program);
- unauthorized blocking, destruction, copying or modification (modification) of computer data;
- neutralization of computer data protection tools;
- means of transmitting, processing and storing protected computer data.

The above-mentioned legal categories are not legally fixed and are not explained in the resolutions of the Plenum of the Supreme Court of the Russian Federation. We also propose to make additions to Chapter 28 of the Criminal Code of the Russian Federation. It is necessary to supplement it with new elements of crimes, for example, Article 272.1 "Illegal possession of a computer information carrier for the purpose of illegal access to computer information" (PARKHOMENKO, EVDOKIMOV, 2015).
In our opinion, it is also advisable to introduce criminal liability for the creation, distribution and use of “botnets”, that is, a network of computer devices and computers infected with malware that makes it possible to remotely control hacked computers and other devices without the knowledge of their owner, as well as use resources for criminal purposes (for example, for anonymous access to the global network, for sending spam, for phishing and Ddos attacks, for cyber-sabotage, for selling drugs, for computer fraud, for committing other crimes). In addition, in order to more effectively and efficiently counteract computer crimes, some researchers propose to add an addition to part 3 of Article 272, part 2 of Article 273, part 1 of Article 274 of the Criminal Code of the Russian Federation, including the following qualifying features:

1. The same acts committed to conceal another crime or to facilitate its commission.
2. The same acts committed to intimidate people or influence the decision-making by local self-government or state authorities, as well as to hinder the normal activities of government bodies, the media, municipal and state enterprises and institutions (MALYKOVTEV, 2006).

It is also recommended to establish a sanction for the above-mentioned acts- imprisonment for up to 10 years. This position is due to the fact that computer crimes are often only a way of committing many other crimes - serious and especially serious (for example, intentional damage or destruction of property; murder; serious injury to health; espionage; extortion; high treason, etc.). We propose to amend Article 151 of the Criminal Procedure Code of the Russian Federation regarding the attribution of crimes provided for in parts 2-4 of Article 272, parts 2-3 of Article 273, parts 1-2 of Article 273. 274 of the Criminal Code of the Russian Federation to the jurisdiction of the FSB of Russia, since these crimes pose a threat to the national security of Russia (EVDOKIMOV, 2015).

Another proposal is to improve judicial practice in criminal cases of computer crimes in Russia. To date, the Plenum of the Supreme Court of the Russian Federation has not formulated explanations regarding the practice of judicial authorities considering criminal cases on computer crimes, which negatively affects judicial and investigative practice. In addition, in most cases, the judicial authorities, passing guilty verdicts, assign to computer criminals types of punishment that do not involve imprisonment (restriction of liberty, suspended sentence, imposition of a fine). This is justified by the fact that computer crimes are acts of medium and small gravity.

Quite often, the judicial authorities assign a penalty that does not involve imprisonment to computer criminals who have had a criminal record for committing criminal offenses. For example, on February 17, 2016, the Kronshhtadtsky District Court of St. Petersburg considered the criminal case of I., previously convicted under Part 1 of Article 322.1 of the Criminal Code of the Russian Federation, accused of committing a crime under Part 1 of Article 273 of the Criminal Code of the Russian Federation, namely, spreading malicious computer programs or other computer information deliberately intended to neutralize computer information protection means. By the verdict of the court And. the sentence was imposed in the form of two years of suspended imprisonment with a probationary period of two years with a fine to the state’s income [Criminal case of the Kronshhtadtsky District Court of St. Petersburg No. 1-26/2016. (http://www.samosud.org/case_756360252).

The analysis of the existing investigative and judicial practice allows us to conclude that the severity and severity of the punishment imposed on citizens who previously had a criminal record and continue to commit cybercrime is insufficient. Of course, this will only contribute to recidivism on the part of computer criminals.

Measures to improve domestic judicial practice require explanations from the Plenum of the Supreme Court of the Russian Federation on issues related to the qualification of acts provided for in Articles 272-274 of the Criminal Code of the Russian Federation. For example, an explanation should be given as to whether the destruction of computer data will be an act in which the data was initially destroyed, but after some time completely or partially restored by specialists? How should the destruction of computer data be qualified by strong high-
frequency or electromagnetic radiation, which did not entail the destruction of the information carrier itself? Should the criminal’s actions be considered as copying computer data when obtaining copies of documents by printing information on a printer, videotaping or photographing images from a PC monitor?

Another measure is to improve and intensify international legal cooperation in preventing and combating computer crimes. Taking into account the cross-border and transnational nature of the crimes under study, the issue related to the interaction of Russian law enforcement agencies with law enforcement agencies of foreign states in the field of countering cybercrime is of great importance (MOROZ, 2018).

Let’s consider an example from judicial practice. So, on 11.11.2017, the Tushinsky District Court of the city of Moscow, for committing criminal acts, responsibility for which is provided for by criminal legislation (part 3 of Article 30, paragraph “b” of part 4 of Article 158, part 3 of Article 272 of the Criminal Code), sentenced the citizens of the Republic of Moldova B. and A. to punishment in the form of imprisonment for a period of 2 years 6 months without paying a fine and without restriction of freedom. The convicted persons will serve the appointed sentence in a correctional colony of the general regime. These persons organized a criminal group and for a long time engaged in skimming in Moscow. They stole money from citizens’ bank cards with the help of special equipment that was installed on the ATM card reader. Some members of the criminal group were able to escape from the investigation outside the Russian Federation [Criminal case of the Tushinsky District Court of Moscow No. 1-520/2017. (https://www.mos-gorsud.ru/rs/tushinskij/services/cases/criminal).

Preventive measures in solving this problem consist in the need to ratify the Convention on Crime in the Field of Computer Information ETS No. 185 of 23.11.2001, to which 47 countries are parties. The official reason is the absence of a special legal norm in the Criminal Code of the Russian Federation, which would provide for criminal liability of legal entities for computer crimes. This circumstance is a serious obstacle to the effective fight against international criminal groups that commit computer crimes on the territory of Russia.

Another measure is to improve the information legislation of Russia. We propose to adopt a federal law on information risk insurance. This law should provide for the insurance of computer data, as well as the means of their transmission, processing and storage against unauthorized blocking, destruction, copying or modification (modification). Before entering into an insurance agreement, the owner (owner) of computer data or means of transmitting, processing and storing protected computer data must install the necessary anti-virus software, which, among other things, will record and prevent unauthorized access. This measure will contribute to reducing the amount of material damage caused, as well as reducing the number of illegal intrusions into computer systems.

It is proposed to consolidate at the legislative level the powers of law enforcement agencies (the FSB, the Ministry of Internal Affairs, the IC, the Prosecutor’s Office of Russia) to exercise control over illegal materials appearing on the network, and, if necessary, allow these bodies to carry out appropriate investigative, operational-search and supervisory measures.

In order to prevent the commission of cybercrimes on the Internet, we propose to fix in Law No. 149-FZ of 27.07.2006 the legal obligation of users of the global network to indicate their personal data (first name, patronymic, surname, date of birth, passport data) when registering web pages and sites, as well as accounts in social networks [Federal Law No. 149-FZ of 27.07.2006 “On Information, Information Technologies and Information Protection” (latest edition). (https://base.garant.ru/12148555/).

The practice of China, where the official personalization of users of the global network was introduced in 2010, shows that this measure has contributed to reducing the number of computer crimes on the Internet several times. Among the most effective special ideological (spiritual and cultural) measures to counter cybercrime, we should highlight:

1. Measures to enhance the activities of the media in the field of preventing computer crimes.
2. Measures to strengthen the legal education of young people.
The main special technical, managerial and organizational measures for the prevention of computer crimes:

1. Measures to train highly qualified specialists in such specialties as "Information Protection" and "Information Security" in higher educational institutions of the Federal Customs Service, the Ministry of Defense, the FSB and the Ministry of Internal Affairs of Russia for the subsequent staffing of law enforcement agencies with competent and professional specialists (TEMIRALIEV, OMAROV, 2019).

2. Measures to create scientific research laboratories in technical universities, research institutes of the Ministry of Internal Affairs, the Federal Customs Service, the Ministry of Defense and the FSB of Russia that would develop and modify software systems for information and computer protection.

3. Measures to create training courses and advanced training courses for employees of financial institutions, organizations, banks, as well as for all interested users of computers and the global network at technical educational organizations.

4. Measures to include in the employment contracts concluded with persons working in the information and telecommunications network and corporate computer system, provisions on personal responsibility for the disclosure of confidential data about the security system of the service computer network.

5. Measures to assign a personal responsibility to the management to monitor the installation and updating of antivirus programs.

6. Measures to ensure close interaction of the internal affairs bodies, the Prosecutor's Office, the FSB of Russia with the media in the prevention and disclosure of computer crimes.

7. Measures to create a national operating system for computers and electronic devices in Russia, as well as to create a nationwide computer system for recording, recording and analyzing computer crimes (the development of such systems can be entrusted to companies such as Group-IB, Kaspersky Lab or Dr. Web).

Forensic measures to prevent computer crime include (ANOSOV, 2018):

1. Improvement of the current criminal procedural legislation of the Russian Federation. As noted earlier, it is necessary to make a number of changes and additions to Article 151 of the Criminal Procedure Code of the Russian Federation. In particular, the crimes provided for in parts 2-4 of Article 272, parts 2-3 of Article 273, parts 1-2 of Article 274 of the Criminal Code should be attributed to the jurisdiction of the FSB of Russia, since cybercrimes increasingly threaten the national security of the state and are of a political nature. It is also proposed to amend articles 176 and 177 of the CPC. It is necessary to determine that the inspection of the scene of the incident, housing, terrain and other premises, documents and objects in order to identify traces of computer crimes, clarify other circumstances that are relevant to the case, should be carried out with the participation of experts.

2. Improvement of existing and creation of new methods for detecting computer crimes with the involvement of experts and specialists in the field of information security (for example, specialists from Dr. Web, Group-IB and Kaspersky Lab can be involved).

3. Generalization and analysis of legal practice by the bodies of the Ministry of Defense, the FSB, the Ministry of Internal Affairs, the IC and the Prosecutor's Office of the Russian Federation in order to develop methodological recommendations on issues related to the investigation and disclosure of cybercrime.

4. The creation of a computer technology and expertise department at each expert forensic center of the Department of Internal Affairs, the Police Department and the
Ministry of Internal Affairs of Russia for the purpose of conducting forensic computer examinations, issuing certificates and conclusions to interested persons.

5. Improvement of training on the basis of the unified training center of forensic experts engaged in the production of forensic computer examinations. Currently, systematic training and advanced training of forensic experts is not carried out in our country. Therefore, there is an urgent need to create a single training center on the basis of the ECC of the Ministry of Internal Affairs of Russia or one of the educational institutions of the Ministry of Internal Affairs of the Russian Federation (for example, in the Volgograd or Omsk Academy of the Ministry of Internal Affairs of Russia).

The list of measures aimed at preventing computer crime can be continued. But, without any doubt, only a comprehensive and integrative approach in the application of preventive measures by law enforcement agencies can significantly increase the level of information security of the Russian Federation and make the prevention of cybercrime more effective. But we should not forget that the proposed preventive measures will be able to give a tangible result only with joint actions of the state with civil society institutions (public associations, mass media, scientific institutions, educational organizations, local self-government bodies, etc.).

In conclusion, we emphasize that the intensive development of IT technologies obliges the state to constantly improve the level of information security of society and strengthen the fight against computer crime. Along with this, the criminal policy in the information sphere should cover a set of measures - organizational, social, economic and other. Of no small importance is the increase in the general and legal culture of the population, the increase in the level of legal awareness of citizens, as well as the strengthening of the effectiveness of the activities of state authorities for the prevention and prevention of computer crimes.

CONCLUSIONS
Summing up the results of the research, we can draw a number of significant conclusions. Having analyzed the existing scientific and regulatory approaches to the state and structure of computer crime in the Russian Federation, we formulated the concept of computer crime in a broad sense.

Computer crime is a set of crimes committed by sane individuals that infringe on the legitimate interests and rights of citizens, organizations, society and the state in the field of safe creation, circulation, protection, receipt, transmission, processing and storage of computer data, the functioning of computer systems and devices, telecommunications, information and other means and systems used for the creation, distribution and practical use of computer data.

The structure of computer crime in Russia includes not only crimes in the field of computer data, but also a significant number of crimes committed with the help of telecommunications and information networks. We emphasize that the number of crimes provided for in Articles 272-273 and 159.6 of the Criminal Code (illegal / unauthorized access to computer data, creation, distribution and use of virus programs, fraud in the field of computer data) will only increase.

The system of computer crimes existing in the current criminal legislation is fundamental for law enforcement practice due to its pragmatism, however, it requires further development by improving the legal features and structures of the elements of crimes. In addition, the current Criminal Code of the Russian Federation should include new crimes that reflect the current needs of criminal legal protection of computer data.

Computer crimes have a certain specificity. The use of technical innovations to commit offenses and crimes allows violators to encroach on the most important public relations in the sphere of interests and rights of the state, society and the individual, protected by law. The complexity of identifying the actions of computer criminals and their capabilities to commit cybercrime increases the degree of social danger of these actions.

On the one hand, computer crime is generated by the same conditions and causes as crime in general. But, on the other hand, it has its own conditions and reasons. In criminology, there is no generally accepted concept of the causes and conditions of crime, including computer crime. This hinders the proper prevention and prevention of the crimes under consideration.
The key conditions and reasons for the growth of computer (cyber) crime are:

1. An increase in the number of crimes in the field of computer software.
2. Improvement of hacker programs.
3. Increasing the intelligence, respectability and professionalism of computer criminals.
4. Complication of the process of studying the identity of the criminal due to the constant rejuvenation of the composition of criminals and an increase in the number of persons who have not previously been brought to criminal responsibility.
5. Huge amounts of material damage caused to the state.
6. The active process of developing computer crime into an international category.
7. High level of secrecy (latency) of computer crimes.

At the present stage, the development and implementation of criminal legal measures to prevent and combat cybercrime are the most important areas of work to ensure an appropriate level of information security of the state and society. Special legal measures to prevent computer crime include activation and improvement of international legal cooperation in the prevention and control of computer (cyber) crimes; editorial revision of the current information and criminal legislation; improvement of domestic judicial practice in criminal cases of cybercrime.

Special ideological (cultural and spiritual) measures to counteract computer (cyber) crimes can be: activation of the media’s activities to prevent cybercrime, as well as strengthening the legal education of the younger generation. Special technical, managerial and organizational measures aimed at the prevention and prevention of computer (cyber) crimes include:

1. Training of specialists in relevant specialties in educational institutions of the Federal Customs Service, the Ministry of Defense, the FSB, the Ministry of Internal Affairs of Russia for the subsequent staffing of law enforcement agencies with competent and professional personnel.
2. Ensuring close interaction and cooperation of the internal affairs bodies, the prosecutor’s Office, the FSB of Russia with the media in the disclosure, prevention and prevention of computer (cyber) crimes.

The number of forensic measures for the prevention and prevention of computer (cyber) crimes include:

1. Improvement of existing and creation of new methods for detecting computer crimes with the involvement of specialists in the field of information security.
2. Creation of specialized departments of computer technologies and expertise in each forensic and expert center of law enforcement agencies for the production of necessary forensic examinations, issuance of certificates and other documents to interested entities.
3. Improvement on the basis of the unified training center for training forensic experts conducting forensic computer examinations.

In conclusion, we note that the list of measures to prevent computer crimes can be supplemented. But only comprehensive and integrative approaches in the application of preventive measures by law enforcement officers can increase the information security of the state, make the prevention and prevention of computer (cyber) crimes more effective. We should not forget that the proposed preventive measures can lead to tangible results only if the state interacts with civil and public institutions (mass media, scientific and educational institutions, public civil associations, local authorities, etc.).
REFERENCES

AL-GARADI, M.A.; VARATHAN K.D.; RAVANA, S.D. Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. *Computers in Human Behavior*, Volume 63, October 2016, p. 433-443.

ANOSOV, A. V. Specially-criminological prevention of crimes committed through the use of high technologies. *Proceedings of the Academy of the interior Ministry of Russia*, 2018, No 4 (48), p. 93-97.

BRINES, J. M. law and the Internet: theoretical problems: dissertation ... Doctors of Law: 12.00.14. Moscow, 2008, 357p.

CHIRKOV, D. K.; SARKISYAN, A. Zh. Crime in the field of telecommunications and computer information as a threat to the national security of the country. *Actual problems of economics and law*, 2013, No. 3, p. 219-226.

CONVENTION ON CRIME IN THE FIELD OF COMPUTER INFORMATION ETS of 23.11.2001 No. 185. Available at: https://base.garant.ru/4089723/. Access: May 21, 2021.

CRIMINAL CASE OF THE KRONSHTADTSKY DISTRICT COURT OF St. Petersburg No. 1-26/2016. http://www.samosud.org/case_756360252. Access: May 21, 2021.

CRIMINAL CASE OF THE TUSHINSKY DISTRICT COURT OF Moscow No. 1-520/2017. https://www.mos-gorsud.ru/rs/tushinskij/services/cases/criminal. Access: May 21, 2021.

CRIMINAL CODE OF THE RUSSIAN FEDERATION No. 63-FZ of 13.06.1996 (as amended on 01.07.2021). Available at: https://base.garant.ru/77683496/. Access: May 21, 2021.

DECREE OF THE PRESIDENT OF THE RUSSIAN FEDERATION No. 537 of 12.05.2009 "On the National Security Strategy of the Russian Federation until 2020". Available at: https://www.garant.ru/products/ipo/prime/doc/95521/. Access: May 21, 2021.

DECREE OF THE PRESIDENT OF THE RUSSIAN FEDERATION No. 646 of 5.12.2016 “On approval of the Information Security Doctrine of the Russian Federation”. Available at: https://www.garant.ru/products/ipo/prime/doc/71456224/. Access: May 21, 2021.

SHOROVSKIKH, L. A. Crimes in the sphere of high technologies. *Cyber-crime*, 2016, No. 4 (28), p. 240-243.

EMIROV, M. B.; SAIDOVO, A.D.; RAGIMKHANOv, D. A. Fighting crimes in global computer networks. *Legal Bulletin of the DSU*, 2011, No. 4, p. 59-62.

EVOKIMOv, K. N. Political factors of computer crime in Russia. *EVOKIMOv, K. N. Information Law*, 2015, No. 1, p. 41-47.

EVOKIMOv, K. N. The structure and state of computer crime in the Russian Federation. *Legal Science and law enforcement practice*, 2016, No. 1 (35), p. 86-94.

FALALEEV, M. A. The damage from cybercrime exceeded 10 billion rubles. https://rg.ru/2019/12/10/mvd-ushcherb-ot-kiberprestuplenij-prevysil-10-miliardov-rublej.html. Access: May 21, 2021.

FEDERAL LAW No. 149-FZ of 27.07.2006 “On Information, Information Technologies and Information Protection" (with amendments and additions). Available at: https://base.garant.ru/12148555/. Access: May 21, 2021.

FROST, N. O. Features of international legal cooperation in the fight against cybercrime in the EU, *Vestnik of the Mari state University*, 2018, No 4 (16), pp. 87-95.

GUNKEL, E. Damage from cybercrime in Russia in 2020 was 69 billion. Available at:
https://www.dw.com/ru/ushherb-ot-kiberprestupnosti-v-rossii/a-56568904. Access: May 21, 2021.

JAHANKHANI H., AL-NEMRAT A., HOSSEINIAN-FAR A. Cybercrime classification and characteristics. Cyber Crime and Cyber Terrorism Investigator’s Handbook. Waltham, 2015. 393p.

JOHN SAMMONS, M. C. Chapter 5 - Cybercrime. The Basics of Cyber Safety, 2017, p. 87-116.

KIMBERLY, A.; DETARDO-BORA, D. J. B. Chapter 8 - Cybercrimes: an overview of contemporary challenges and impending threats. Digital Forensics, 2016, p. 119-132.

KOCHKINA, E. L. Definition of the concept of “Cybercrime”. Certain types of cybercrimes. Siberian criminal procedural and criminalistic readings, 2017, No. 3 (17), p. 162-169.

KOMAROV, A. A. On the criteria of public danger, crimes in the field of high technologies. Actual issues of law, economics and management: collection of articles of the IX international scientific and practical conference. Penza, 2017, p. 243-245.

MALYKOVTEV, M. M. Criminal liability for the creation, use and distribution of malicious computer programs: dis. ... cand. yurid. M.: RSE, 2006, 186p.

NOMOKONOV, V. A.; TROPINA, T. L. Cybercrime: forecasts and issues of struggle, the Library criminologist, 2013, No 5 (10), p. 148-160.

PARKHOMENKO, S. V., EVDOKIMOVO, K. N. Prevention of computer crime in the Russian Federation: an integrative and comprehensive approaches. Russian criminological journal, 2015, no. 2, p. 265-275.

PETROVA, I. A.; LOBACHEV, A. I. Crimes in the field of computer (digital) information: debating the issues of defining the concept, the object of criminal legal protection of and the subject of the abuse, Journal of applied research, 2020, no. 1, p. 52-62.

TEMIRALIEV, T. S.; OMAROV, E. A. Problems of countering crimes committed with the use of information systems and ways to solve them. Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan, 2019, No. 1 (55), p. 93-99.

VORONOV, So Russia could lose up to 3.6 trillion rubles due to cybercrime in 2020 - “Sberbank”. Available at: https://www.finam.ru/analysis/newsitem/rossiya-mogla-poteryat-do-3-6-trln-rubleiy-iz-za-kiberprestupleniy-v-2020-godu-sberbank-20201228-163126/. Access: May 21, 2021.

YERJANOV, T. K. et al. Legal Issues Related to Combating Cybercrime: Experience of the Republic of Kazakhstan. Journal of Advanced Research in Law and Economics, [S.l.], v. 8, n. 7, dec. 2017, p. 2276-2291.
Crime prevention in the field of computer technologies at the present stage in the Russian Federation: problems and ways to solve them

Prevenção ao crime no campo das tecnologias computacional na atual fase na Federação Russa: problemas e formas de resolvê-los

Prevenção del delito en la esfera de las tecnologías informáticas en la etapa actual en la Federación de Rusia: problemas y formas de resolverlos

Resumo
No artigo, baseado na análise das abordagens existentes ao Estado e na estrutura do crime computacional na Federação Russa, os autores formularam o conceito de "crime computacional", identificaram as principais características desse tipo de crime; e também, com base na análise das causas e condições de cometimento de crimes no campo das altas tecnologias, desenvolveu um conjunto de medidas legais especiais, ideológicas, gerenciais, organizacionais e forenses que visam prevenir e prevenir crimes de informática. Alontseva Dina Viktorovna; Lavrishcheva Olga Anatolyevna No decorrer desta pesquisa, foram estudadas as normas de atos internacionais, legislação interna, relatórios e estatísticas de agências de aplicação da lei da Federação Russa e organizações especializadas, materiais de prática judicial, bem como fontes doutrinárias sobre o tema do trabalho. Os autores utilizaram métodos gerais de cognição científica (dialectica, inductiva, deductiva), bem como métodos científicos privados utilizados nas ciências jurídicas - o método do direito comparativo e o método jurídico formal.

Keywords: IT technologies. Computer crimes. Russian legislation. Law enforcement practice. Information and telecommunications networks.

Palavras-chave: Tecnologias de TI. Crimes de computador. Legislação russa. Prática de aplicação da lei. Redes de informação e telecomunicações.

Abstract
In the article, based on the analysis of existing approaches to the state and structure of computer crime in the Russian Federation, the authors formulated the concept of "computer crime", identified the key features of this type of crime; and also, based on the analysis of the causes and conditions of committing crimes in the field of high technologies, developed a set of special legal, ideological, managerial, organizational and forensic measures that are aimed at preventing and preventing computer crimes. Alontseva Dina Viktorovna; Lavrishcheva Olga Anatolyevna In the course of this research, the norms of international acts, domestic legislation, reports and statistics of law enforcement agencies of the Russian Federation and specialized organizations, materials of judicial practice were studied, as well as doctrinal sources on the topic of the work were analyzed. The authors used general methods of scientific cognition (dialectical, inductive, deductive), as well as private scientific methods used in the legal sciences-the method of comparative law and the formal legal method.

Resumen
En el artículo, basado en el análisis de los enfoques existentes sobre el estado y la estructura de los delitos informáticos en la Federación de Rusia, los autores formularon el concepto de "delito informático", identificaron las características clave de este tipo de delito; y también, a partir del análisis de las causas y condiciones de la comisión de delitos en el ámbito de las altas tecnologías, se elaboró un conjunto de medidas jurídicas, ideológicas, de gestión, organizativas y forenses especiales encaminadas a prevenir y prevenir los delitos informáticos. Alontseva Dina Viktorovna; Lavrishcheva Olga Anatolyevna En el curso de esta investigación, se estudian las normas de los actos internacionales, la legislación nacional, los informes y las estadísticas de los organismos encargados de hacer cumplir la ley de la Federación de Rusia y las organizaciones especializadas, los materiales de la práctica judicial, así como las fuentes doctrinales sobre el tema de la obra. Los autores utilizaron métodos generales de cognición científica (dialectica, inductiva, deductiva), así como métodos científicos privados utilizados en las ciencias jurídicas-el método de derecho comparado y el método legal formal.

Palabras-clave: IT tecnologías de la información. Delitos informáticos. Legislación rusa. Prácticas policiales. Redes de información y telecomunicaciones.