Criminalistics specifics of methods of committing computer crimes and peculiarities of their prevention

Características de los métodos de criminalística para cometer delitos informáticos y peculiaridades de su prevención

Vitaliy Polyakov[1]
Altai State University - Russia
agupolyakov@gmail.com

ABSTRACT

The article develops a new approach to computer crime, which consists in the forensic differentiation of methods of committing computer crimes by their complexity and danger level. We revealed the characteristic features of different types of computer crimes and classified the means and receptions of hi-tech ways of committing computer crimes, namely cyberterrorism, cyber-extremism and illegal influence on state critical information infrastructure. A new methodology for the forensic prevention of computer crimes has been proposed, based on the application of Honeypot technology. The results of the work allow to develop the modern criminalistic theory of crimes in the sphere of computer information, while data obtained during the research can be used as a scientific basis for conducting investigations of computer crimes.

Keywords: Method of committing crimes, forensic characterization, computer crimes, crime prevention.

RESUMEN

El artículo desarrolla un nuevo enfoque para el delito informático, que consiste en la diferenciación forense de los métodos para cometer delitos informáticos por su complejidad y nivel de peligro. Revelamos las características de los diferentes tipos de delitos informáticos y clasificamos los medios y las recepciones de las formas de alta tecnología para cometer delitos informáticos, a saber, el ciberterrorismo, el ciber-extremismo y la influencia ilegal en la infraestructura de información crítica del estado. Se ha propuesto una nueva metodología para la prevención forense de los delitos informáticos, basada en la aplicación de la tecnología Honeypot. Los resultados del trabajo permiten desarrollar la teoría criminalista moderna de los delitos en el ámbito de la información informática, mientras que los datos obtenidos durante la investigación pueden utilizarse como base científica para realizar investigaciones de delitos informáticos.

Palabras clave: Método de cometer delitos, caracterización forense, delitos informáticos, prevención del delito.

1 PhD, Associate Professor, Department of Criminal Procedure and Criminalistics, Altai State University, Russian Federaion.

Recibido: 17/06/2019 Aceptado: 19/10/2019

INTRODUCTION

Modern society increasingly depends on information stored and used in electronic form and disseminated through information networks. Such information has insufficient legal, technical and organizational protection against rapidly increasing quantitative and qualitative changes in computer crime that encroaches upon it. Such crimes pose a serious threat to individuals, organizations and institutions, to the State as a whole. Existing forensic knowledge has proved insufficient to combat a fundamentally new and specific type of crime (Diamon and Bachmann, 2015). As a result, the causes and conditions contributing to the commission of these crimes were not identified, no forensic characteristics for their main types were formed, no specific features and difficulties of proof were identified, and, in fact, no effective measures for the forensic prevention of these crimes were proposed. The difficulty of solving these problems is largely determined by the fact that traditional criminalistics methods proved to be inadequate to the rapid development of complex and dangerous methods of committing computer crimes related to the professional organized activities of criminal groups, using the latest advances in scientific and technological advances in the field of software and hardware capabilities of computer equipment and telecommunications systems. These circumstances determine the high relevance of the topic devoted to the study of patterns of committing and investigating crimes in the field of computer information.

In the article on the basis of the analysis and generalization of available investigatory and judicial practice the new approach to the given kind of crimes, consisting in criminalistic differentiation of ways of their fulfillment develops. A new type of classification of methods of committing computer crimes by their complexity and danger level is proposed. This creates an opportunity for scientific and practical purposes to introduce new concepts - relatively simple methods of committing these crimes and high-tech methods of committing computer crimes. The necessity of introduction of hi-tech methods of committing computer crimes into the Criminal Code of the Russian Federation with the purpose of aggravation of responsibility is substantiated. An important and new feature of modern criminalistics is the identification of the causes, conditions and circumstances that contribute to the commission of computer crimes and complicate their investigation. For the first time, a methodology has been developed for the forensic prevention of the main types of computer crimes that have been delineated by the method of committing them.

Author's positions develop the criminalistic theory, being a scientific base for struggle against computer crimes. These provisions contribute to the acquisition of new forensic knowledge, providing the formation of the initial part of the investigation methods of high-tech computer crimes. The results of the research will make it possible to develop the existing and create new and more effective methods and techniques of computer crime investigation.

Objectives of the study

The main purpose of this work is the forensic investigation of methods of committing computer crimes. Within the limits of this research the concrete problem of an establishment of the separate groups of the computer crimes divided on criminalistic complexity and public danger of ways of their fulfillment is solved. Specific proposals for the prevention of crimes committed by different means are developed for the selected groups. Central to the solution of this problem is the study of the peculiarities of committing the most dangerous high-tech crimes. An important task is also the development of a new methodology for the prevention of crimes in the area of computer information.

DEVELOPMENT

Methods

The research is based on a set of methods and techniques used in modern forensics. The research methodology included such general scientific methods as method, abstraction method, analogy method, generalization method, formal logic method and others. The method of collecting and analyzing empirical material and the statistical method for its processing and generalization were also used. A formal legal method was used to analyse the existing legal framework for computer-related crime, a specific sociological method to study the effectiveness of legal institutions in countering computer-related crime and an expert assessment method. The research was conducted on the basis of the principle of consistency (consideration of the phenomena under study as a set of elements ordered in space and time) and the principle of truthfulness (reliability of new knowledge).

In the course of the work, the materials of forensic research describing who, where, when, in what way, in what environment and by what means commit computer crimes were collected and summarized. The materials of judicial and investigative practice of investigating computer crimes, as well as some other crimes committed with the use of information technologies, were collected and analyzed. Original questionnaires were conducted among representatives of various categories of law enforcement agencies, experts and specialists in information technology and information security. The tools used included a set of specially prepared documents that were used to collect empirical information on computer crimes: questionnaires and questionnaires for law enforcement officials and professionals, and expert assessment matrices. The toolkit also included mathematical methods for processing digital (statistical) data. The questionnaires were statistically processed, analysed and synthesized.

On the basis of the collected data, a new approach to the study of computer crimes was proposed and justified, namely, the creation of a forensic classification of computer crimes by mode of commission. This approach made it possible to make a forensic distinction between crimes in the field of computer security by the level of their technological complexity and public danger, which ensured the creation of original forensic characteristics separately for each group of methods of committing them. The materials obtained were also used to develop a criminalistics framework for individual types of computer crimes, classified according to the modus operandi.

Results and discussion

The patterns of commission and classification of different types of computer crimes. Methods of committing crimes in the field of computer information have their own characteristics, which allows them to be classified according to technological complexity and social danger. The importance of this task is related to the fact that law enforcement practices in the investigation of different crimes in the field of computer information differ significantly. This fact confirms the need to identify subtypes or subgroups within one type of crime. Such differentiation will make it possible to improve the legislative regulation of these crimes, as well as to adjust the existing methods of detection, investigation and prevention of crimes.

All crimes involving the use of information technology can be classified as relatively simple and high-tech crimes.

Table 1. Classification of computer and communication equipment

1. By type of property	1.1. Personal
	1.2. Public
2. By type of mobility of means of committing crimes	2.1. Mobile
	2.2. Stationery
3. By the nature of construction of the communication channel	3.1. Direct connection channel
	3.2. Indirect connection channel
4. Computer information detection in the energy-dependent part of the device	4.1. Non-volatile devices
	4.2. Energy-dependent devices

Relatively simple methods cause less difficulties in practice, but they are investigated with many investigative errors. These errors have been analyzed and used to develop effective forensic recommendations (Polyakov, 2016). Relatively simple ways to access computer information remotely and unlawfully are typified into the following groups: gaining access by exploiting vulnerabilities and errors in software development; gaining access through the negligence or negligence of the victims themselves; and gaining access through the use of special malicious software.

High-tech techniques have a number of specific features that, taken together, create a new quality that makes such crimes virtually undetectable (latent) and, when they come to the attention of law enforcement authorities, do not give rise to criminal proceedings or will soon be discontinued.

When investigating high-tech computer crimes committed remotely through information networks, special attention should be paid to the detection of crime traces. These, in our opinion, can be divided into the following groups of indicators for forensic purposes (Polyakov, Kurakin, 2018):

- By type of property - personal and public. For example, public communication devices allow for their use under specific conditions and circumstances, and usually contain traces of communication between different individuals (identification features belonging to different individuals at different times) (Meshcheryakov, 2004);

- In terms of mobility, mobile and stationary. For example, mobile means of remotely committing crimes while in working order change their location, leaving traces of movement in space from one base station (BTS) to another;

- By the nature of the communication channel - a direct connection channel and an indirect connection channel). Thus, for example, an indirect connection channel differs in the presence of traces of network interaction not only in the connecting devices, but also on the computer equipment of connection intermediaries: routers, routers, gateways, servers and other network equipment;

- Energy dependence of the device in which the information is stored - non-volatile devices and energy-dependent devices. The collection of forensic computer information should begin with the energy-dependent part of the devices, which is explained by the risk of losing it due to possible actions to conceal the traces of crime and counteract the investigation by criminals who have established mechanisms of information destruction or send commands remotely.

Computer equipment and communication devices, which are important for the investigation, can be presented in the form of Table 1 for ease of use for forensic purposes.

Criminally significant features of high-tech methods of committing computer crimes. Let us consider in more detail the methods of committing the most dangerous types of crimes in which information technologies are actively used. These include high-technology crime, cyberterrorism, cyber-extremism and undue influence on the critical information infrastructure of a state.

Investigators face significant challenges in investigating crimes that are committed by technically sophisticated means using information technology. The prospect of such criminal cases being brought to trial is often low. The reason for this is largely due to the specific nature of the crimes, namely, the complexity of the methods of committing them

through the use of different methods of concealing the traces of crimes.

It should be noted that the number of effective software and hardware and computer crime concealment technologies increases every year, along with their availability, which increases the problem. The fight against this phenomenon remains ineffective today. For example, an attempt to block the popular messenger "Telegram", which can be used in criminal activities, due to the complexity of control over the information circulating through it, has led to the mass use of proxy servers that replace the IP-address of mobile devices and bypass the blocking of this messenger by Roskomnadzor.

The greatest difficulties arise in the investigation of crimes committed by professional criminals in technically and organizationally complex ways. Such crimes are often the most dangerous to society (Raed, Faqir, 2013). Analysis of forensic literature, judicial and investigative practices and questionnaires among law enforcement officials, experts and information technology specialists has allowed for the definition of these crimes and the introduction of a new concept - high-tech crimes.

Let's define the features and criminally significant features of high-tech crimes. Their main feature that is criminally significant is the fact that they have many similarities with computer crimes in their commission and investigation. The most important forensic indicators of high-tech crime are contained in the personality traits of criminals who are computer and information specialists, who are grouped together in criminal groups and communities to achieve their criminal goals (Broadhurst et al., 2014). It should be noted that the group may not have the technical expertise of all participants. The use of specially designed or modified software or hardware and software tools for criminal purposes is essential for high-tech methods of committing crimes. This requires criminals to have in-depth technical knowledge and practical programming skills. The complexity of these crimes is evident in the fact that the way in which they are committed, in terms of criminality, is fully structured. As already noted, the direct commission of crimes is preceded by a preparatory stage. However, in addition to the preparation and commission of the offence, a special role is given to the early identification of opportunities to conceal and destroy traces of criminal activity.

The commission of high-tech crimes involves the use of networked telecommunications technologies. These technologies are an integral part of the modus operandi of these crimes, making it possible to carry out unauthorized access to computer information, cyberterrorism, cyber-extremism and other crimes.

High-tech crimes have extremely negative consequences for society, which consist in causing significant harm to someone else's interests or in creating a real threat of such harm. In many cases, this is the purpose of the criminal intent, i.e., the criminals are cynical about the values of information society. These features or elements of the criminal characteristics of the crimes in question, which are not directly related to the method, but are dependent on it, show the increased public danger of such crimes. In our opinion, it is necessary to take into account at qualification, having fixed at legislative level as a separate crime or an aggravating attribute of crimes, for example, provided by article 272 of the Criminal Code of the Russian Federation "Illegal access to computer information".

High public danger of a part of computer crimes provoked the legislator to add a new composition provided by Article 274.1 of the Criminal Code of the Russian Federation "Unlawful influence on the critical information infrastructure of the Russian Federation". In our opinion, the appearance of Article 274.1 of the Criminal Code of the Russian Federation is one of the manifestations of an adequate response to high-tech crimes, but such a response is incomplete due to a fragmented approach to a broader phenomenon. We believe that it is more expedient to define high-tech crimes and to use this category in various existing elements of crimes, which may include its features. This also applies to new compositions that will appear in the future, for example, in connection with the emergence of information technologies (in particular, computer programs and devices) operating on the principle of artificial intelligence.

Crimes committed by high-tech methods are based on separate techniques, which in most cases are typical, but can also be quite rare or even unique. Depending on the peculiarities of such methods or their combinations, it is advisable to divide all high-tech methods into groups for scientific and practical purposes. The criterion for classification of these methods is the specificity of the methods used for their performance and concealment. On the basis of this criterion, the following types of high-tech crimes can be identified.

1. Using special programs for remote computer control. In this case, access to certain network resources is usually obtained. Thus access to the object of infringement is carried out from other network or the terminal which is not constantly connected with it physically or logically. The most popular programs for remote management: "Radmin", "TeamViewer", "AeroAdmin" (Polyakov, Lapin, 2014).

2. Techniques based on encryption of the processes performed and traces of impact on computer information left behind.

> 2.1 Encryption of any data or operations on computer equipment or remote service. This can be done, for example, by using an external storage device with a secure special operating system, which will store most of the traces of the operations performed.
>
> 2.2 Close to the previous reception is the encryption of traffic, which can be carried out with the help of different software and technologies. For this purpose anonymous networks are used, for example, "P2P", "Freenet" and others.

3. A technique based on other technology and software, but also used to hide network activity, is the use of a virtual private VPN network. Such a network is usually a geographically distributed private logical network based on existing networks with similar or similar parameters and services to the core network. VPN networks have a fairly high level of data protection.

4. use of so-called anonymizers, the task of which is to mask the IP-addresses of devices, the lack of information about them and the connections made by them on the Internet.

5. Use of "virtual machines" ("hypervisors"). The number of corresponding programs increases every year, and VirtualBox and VMWare virtual machines are popular among them today.

6. Use of dedicated servers (on the slang of "dedicators"). In this technique, the remote connection is made through a dedicated server, which can be located quite far away, including in another country, which allows you to hide the traces of crime by means of anonymization, building a specific routing from specific IP-addresses and on the counteragent ports when connecting to the server.

Summarizing all the above, we can formulate two concepts of high-tech crime. The first is necessary for the criminal law, as it allows us to propose a new set of crimes or to add an aggravating feature to the relevant crimes, for example, in Article 272 of the Criminal Code of the Russian Federation "Illegal access to computer information". The second concept corresponds to the tasks of criminalistics and contains significant features for this science, which will allow more effective investigation and prevention of such crimes.

In criminal law, crimes committed with the help of specially created or modified software, hardware and software or hardware using information networks should be considered as high-tech crimes, as a result of which significant damage to someone's interests is inflicted or there is a real threat of its occurrence.

In forensic science, high-tech crimes are crimes committed in a group form in a fully-structured manner by original means using information networks, which objectively predetermines the forensic complexity of their investigation.

Methods of committing cyberterrorism and cyber-extremism. It should be noted that, in recent years, forensic theory has made significant progress in the study of methods of committing crimes in the area of computer information. However, processes influenced by scientific and technological progress are constantly changing not only computer crime, but also traditional crime, introducing new techniques based on the use of computer equipment and technologies into the means of achieving criminal results. In this regard, in recent years, it has become relevant to study computer-based methods of committing dangerous crimes such as terrorism (Cameron, 2015) and extremism (Sunami, 2013).

A manifestation of these methods is the organization of the activities of a terrorist organization and participation in the activities of such an organization (Article 205.5 of the Criminal Code of the Russian Federation), which are carried out with the use of information and telecommunication technologies, for example, for communication between members of the organization, excluding visual and sound personification of a person. It can be argued that terrorism and extremism have now ceased to exist only in their usual form, with new manifestations - cyberterrorism and cyber-extremism.

Cyber terrorism, unlike traditional terrorism, is linked to the use of information and communications technology and is most often carried out by criminal groups, both for the purpose of organizing their activities and directly for the preparation and commission of acts of terrorism. The use of telecommunications networks offers criminals a number of advantages. For example, access to information resources is facilitated, regardless of the geographical location of the perpetrators and their victims; there is a significant audience of recipients of terrorist appeals; there is a high speed and volume of information transmitted; and information is transmitted through channels of communication that are virtually uncontrolled by law enforcement authorities.

The criminal manifestations of cyberterrorism can vary, most notably

1. The most dangerous manifestation of cyberterrorism is the terrorist act (article 205 of the Criminal Code) carried out against the critical information infrastructure of the State.

2. Cyberterrorism may be carried out through the use of information technologies to induce, recruit and otherwise involve persons in terrorist activities (article 205.1 of the Criminal Code).

3. Another manifestation of cyberterrorism may be a call for terrorist activities, a public justification of terrorism or its propaganda (article 205.2 of the Criminal Code), carried out in the following ways

- Mass spam mailing, which is a non-personified and, as a rule, anonymous letter with a peculiar advertising and propaganda character;

- By sending out an e-mail with an invitation to join a terrorist organization to persons previously selected on certain principles who may adhere to antisocial views;

- Posting calls for terrorist activities in photo, audio, video and text file formats on various Internet

resources (social networks, blogs, forums and other publicly accessible websites);

- Hacking into popular websites and leaving propaganda messages there.

Information technologies are also used to maximize the "immersion" in the atmosphere of intolerance towards other people's views, in particular through distance learning for the purpose of carrying out terrorist activities (article 205.3 of the Criminal Code).

Cyber-extremism uses web-based information technologies to interact with members of extremist communities, propagandize and agitate their actions, recruit new participants, send out information about "white patrols", counter-system "flashmobs", finance the activities of banned organizations, etc. (Polyakov, 2016). Cyber-extremism uses web-based information technology in the following ways:

- Mailing (direct mail), which includes sending invitations to join extremist organizations to Internet users, or sending them propaganda information on extremist content, such as the time and place of extremist "flash mobs";

- Spamming differs from the previous method in that it involves anonymous, non-personalized mass emails, usually of an advertising nature;

- Dissemination on the Internet (on social networks, blogs, forums and other public websites) of extremist content in photographic, audio, video and text file formats with relevant appeals, inducements or endorsements of extremist activities.

Individuals committing extremist crimes using the Internet usually use the following techniques to conceal the electronic digital traces of their participation in them and to otherwise counteract them (Osipenko, 2010) to law enforcement agencies:

1) Specify someone else's or fictitious registration, identification and record data;

2) Delete data files that contain information on criminal activity, such as social networking user accounts, created or modified programs that produced extremist materials, logs of changes in the operating system, etc;

3) Use anonymous proxy servers, firewalls, specialized software that allows to substitute information about IP-address, MAC-address, geopositioning (Semenov, 2004);

4) Remailers and anonymizers (e.g. TorBrowser) are used to forward e-mails from another computer, to change the sender's return address and e-mail service.

Ways of improperly influencing critical information infrastructure. At present, the issues of preparation, commission and concealment of crimes under Art. 274.1. The Criminal Code of the Russian Federation (improper influence on critical information infrastructure).

Methods of committing crimes for each of the three traditional forms of criminal attacks on the security of computer data and systems under domestic law are delineated as follows

1) Creation, use and distribution of malicious software;

2) Illegal access to computer information;

3) Violation of rules of operation of means of storage, processing or transfer of computer information.

Examples may be given for each form of criminal offence against the security of computer data and systems. For example, malware may be distributed either through the distribution of computer media containing such media (floppy diskettes, CDs, flash cards) or in ways unrelated to the circulation of media, such as e-mail, the Internet, the local area network and remote access to the system (Holt. Th.J. et al., 2012). Methods of obtaining illegal access to information on crimes under Article 274.1 of the Criminal Code of the Russian Federation are subdivided into access through the use of vulnerabilities and mistakes made in the development of software (by launching malicious software from packers that bypass the protection of anti-virus systems; access as a result of negligence or negligence of the victims themselves accessed through the use of special, including malicious, software.

In the process of concealment, the groups of actions of the offender in relation to computer information on crimes provided for by Article 274.1 of the Criminal Code of the Russian Federation can be divided into concealment by concealing information, concealment by destroying information, concealment by masking information and concealment by falsification of information. It should be noted that the study of crimes provided for by Article VI of the Criminal Code of the Russian Federation, as well as the investigation of crimes provided for by Article VI of the Criminal Code of the Russian Federation, are carried out by the Ministry of Internal Affairs of the Russian Federation. 274.1. The Criminal Code of the Russian Federation is one of the topical tasks of modern forensics.

Fundamentals of methodology of prevention of computer crimes. The specific task of forensic crime prevention is to improve scientific and technical means, tactical methods and methods of investigation, which increase the efficiency

and scientific and methodological level of investigation as a whole. The development of measures to suppress the crime that has begun and is being prepared is one of the private tasks of forensic prevention. In criminal science, the possible commission of crimes may be hindered by legal measures, such as acts of prosecutorial response, or by technical methods and means that can be used to suppress the crime. The notion of "suppression of crime" in some ways reflects the results of prevention and implies that law enforcement agencies are directly involved in practical activities to eliminate existing events with socially dangerous consequences (Conradt, 2012). Crimes that are usually of a continuous or episodic nature are suppressed in criminal terms.

At present, computer crimes are practically not countered by means of forensic prevention. This makes it important to develop a system of measures to counter computer crime that takes into account its structure, trends and different criminal situations. All measures of criminalistic prevention of computer crimes should be divided into legal, technical, organizational and methodological measures. To increase their effectiveness, these measures should be implemented in combination, i.e. (Parkhomenko and Evdokimov, 2015).

An important aspect of the system of prevention measures is the division of these measures into two large groups, namely, those related to crimes committed by relatively simple methods and the most dangerous high-tech methods. The group of legal measures includes changes and improvements to the existing legislation, while improvement of both substantive and procedural law is equally important. In our view, it is necessary to include increased liability for crimes committed by high-tech methods as compared to relatively simple crimes. It is necessary to exercise more control over the developers of computer programs, encryption tools, software and hardware information security devices.

Organizational measures can be divided into two groups: improving the work of law enforcement agencies (Pastukhov, Losavio, 2017) and protection from computer crimes organizations. Organizational measures aimed at improving the work of law enforcement agencies should include addressing the problems of interaction between the structures providing for the investigation of computer crimes. Such interaction should involve not only state and public bodies and organizations of Russia, but also work with organizations of other states.

In the area of methodological measures, an original methodology could be proposed based on the use of Honeypot technology to gather forensic information, including for the preventive search for potential criminals and targets, new and complex methods and means of committing crimes (Howell, C.J., et al., 2017; Polyakov, 2017). The use of this technology makes it possible to identify previously unknown features of high-tech crimes committed with the use of modern technologies, in particular, by means of the TOR system, anonymous proxy servers, VPN services and other technologies for concealing traces of criminal activity.

We also believe that at present, the introduction of artificial intelligence technology into criminal activities to counter the most dangerous crimes in which information technology is used is becoming increasingly popular. The main directions of research and application of artificial intelligence technologies in forensics are the following: forensic analysis of crimes committed by means of artificial intelligence technologies; development of technical, tactical, methodological recommendations for investigation of crimes committed by means of artificial intelligence technologies; development of new methodological approaches to the investigation of crimes; increasing the potential of traditional expert studies; prevention of adversaries.

In forensics, the issue of whether the subject of crime prevention through legal education and information of citizens is included in its subject matter is debatable. Until recently, the issues of education in criminalistics were absent even in the staging, the subjects and object of this activity were not defined, there were no studies of the forms, techniques and methods of its implementation. We believe that education and information of citizens can take a relatively independent place in criminalistics (Garmaev, Popova, 2016) and, therefore, can be used as a component of methodological measures to prevent computer crimes.

Technical prevention measures relate to the development and use of software and hardware and information protection methods and tools. It should also be noted that the comprehensive application of the system of criminalistic prevention of computer crime should first of all help to reduce the number of the most dangerous types of computer crime.

CONCLUSIONS

The paper proposes a new approach to forensic investigation of computer crimes, based on the identification of characteristic methods of their commission. On the basis of the collected and generalized judicial practice, as well as the conducted survey of law enforcement officers and specialists, the characteristic features of committing crimes in the field of computer information are revealed. A new classification of the crimes under study has been developed, based on the consideration of their technological complexity and social danger.

The division of computer crimes into two groups is justified: relatively simple crimes and crimes committed by high-tech methods.

Criminalistics features of high-tech methods of committing computer crimes are determined. It is shown that the most important of them are the use of specially created or modified for criminal purposes software and hardware and software, remote committing of crimes with the use of network technologies, specific preparation for the crime, which consists in concealment of electronic digital traces. The means and methods used in high-tech methods of committing crimes are classified.

Methods of committing such dangerous types of computer crimes as cyberterrorism, cyber-extremism and undue influence on the critical information infrastructure of the state have been studied.

A new methodology for the forensic prevention of computer crimes, including legal, organizational, methodological and technical measures and adapted to the specifics of different methods of committing crimes, is considered. The method of collection of criminally significant information and preventive search of potential criminals and objects of their encroachments based on the application of Honeypot technology is proposed.

The positions developed in the article develop the forensic theory and can be used as a scientific basis for investigation of computer crimes. The results of the research can also be used to create a comprehensive methodology for the forensic prevention of computer crimes committed in different ways.

BIBLIOGRAPHIC REFERENCES

Broadhurst, R. Grabosky, P., Alazab, M. & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime International Journal of Cyber Criminology, 8(1), 1-20.

Cameron, S. D. (2015). Brown. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice // International Journal of Cyber Criminology. Vol. 9 (1): 55–119. DOI: 10.5281/zenodo.22387

Conradt C. (2012). Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case. International Journal of Cyber Criminology (IJCC), 6(1), 912-923.

Diamon, B., Bachmann, M. (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. International Journal of Cyber Criminology, 9(1), 24–34. DOI: 10.5281/zenodo.22196.

Garmaev, Y.P., Popova, E.I. (2016). The Organization of Anticriminal and Antiterrorist Education in the Crimean Federal District. Criminology Journal of Baikal National University of Economics and Law, 2016, 10(2), 270-279.

Holt, Th.J., Strumsky, D., Smirnova, O., Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. International Journal of Cyber Criminology, 6(1), 891-903.

Howell, C.J., Maimon, D., Cochran, J.K., Jones, H.M., Powers, R.A. (2017). System Trespasser Behavior after Exposure to Warning Messages at a Chinese Computer Network: An Examination. International Journal of Cyber Criminology, 11(1), 63–77. DOI: 10.5281/zenodo.495772.

Meshcheryakov, V.A. (2004). Electronic Digital Objects in Criminal Proceedings and Forensics. Voronezh Forensic Readings: Research Collected Works, 5, 153-169.

Osipenko, A.L. (2010). Operative-search activity in cyberspace: answers to new challenges. Scientific Bulletin of the Omsk Academy of the Russian Ministry of Internal Affairs, 2(37), 38-43.

Parkhomenko, S.V. Evdokimov, K.N. (2015). Computer Crime Prevention in the Russian Federation: Integrative and Integrated Approaches / S.V. Parkhomenko, K.N. Evdokimov. Criminological Journal of Baikal State University of Economics and Law, 2, 265-276.

Pastukhov, P.S., Losavio, M. (2017). Ispol'zovanie informatsionnykh tekhnologiy dlya obespecheniya bezopasnosti lichnosti, obshchestva I gosudarstva [Use of Information Technology to Ensure Security of the Individual, Society and State]. Vestnik Permskogo Universiteta. Juridicheskie Nauki - Perm University Herald. Juridical Sciences, 36, 231–236. DOI:10.17072/1995-4190-2017-36-231-236.

Polyakov, V.V. (2016). Forensic analysis of relatively simple ways of committing computer crimes. South Ural Forensic Readings: Collection of Reports of All-Russian Scientific-Practical Conference. Ufa: RIC BashGU.

Polyakov, V.V. (2016). Prevention of extremism and terrorism through the Internet. Izvestia of Altai State University, 3(91), 142-144.

Polyakov, V.V. (2017). The honeypot system as an information gathering tool to combat cybercrime. Forensic science library, 1(30), 250-254.

Polyakov, V.V., Kurakin, A.V. (2018). Investigation situations of the initial stage of investigation of computer crimes committed remotely. Problems of legal and technical protection of information, 6, 113-119.

Polyakov, V.V., Lapin, S.A. (2014). Means of committing computer crimes. Reports of the Tomsk State University of Control Systems and Radioelectronics, 2(32), 162-166.

Raed, S. A. Faqir (2013). Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No.30 of 2010. International Journal of Cyber Criminology, 7(1), 81-90.

Semenov, A.Yu. (2004). Some Aspects of Detection, Seizure and Investigation of Traces of Computer-related Information Crime. Siberian Legal Gazette, 1.

Stratton, G., Powell, A. and Cameron, R (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? International Journal for Crime, Justice and Social Democracy, 6(2), 17-33. DOI: 10.5204/ijcjsd.v6i2/355.

Sunami, A.N. (2013). Youth Extremism, Xenophobia, Intolerant Behavior: Conflict Analysis of the Russian Internet. Conflictology, 1, 178-185.