Alizada C. Sh., Aliyev B.A.[♦]

Detection, fixation and acquisition of physically useful information in a computer network

Abstract: One of the most troubling issues in the globalization era is the issue of security and its provision.It is now possible to note that cyber security is becoming a strategic national issue that affects all levels of government and society.

In recent years, information and communication technologies (ICTs) develop so rapidly that it is often impossible to predetermine its subsequent consequences, and it is necessary to spend enough time, knowledge and knowledge to overcome the resulting negative situation. Basically, the new technologies, projects and programs that are used in the Internet global network seem to be beneficial and harmless at first, but experience shows that in many cases, it is impossible to get them completely.

The expansion of computer networks promotes the broader use of network technology capabilities in cyberspace, and enhances coordination, coverage and complexity in networking activities.This leads to the multiplication of cybercrime, by the users who are equipped with more advanced and modern ICT tools.

Based on the above, we can say that ensuring cyber crime is a vital issue. A national policy on this issue and a cyber security strategy that is developed within this policy is required. As cyber attacks are likely to result in tangible and even possible consequences, cyber security is of great importance in determining and punishing those results and actions and methods that result in these consequences.

[♦] **Alizada Cavid Shirzad oglu –** Researcher of “The legal provision of state security” of the Institute on Law and Human Rights of the Azerbaijan National Academy of Sciences (Azerbaijan). E-mail: cavid6455@mail.ru

Aliyev Bakhtiyar Abdurahman oglu – PhD in Law, Associate Professor, Head of the Department of “The legal provision of state security” Institute on Law and Human Rights of the Azerbaijan National Academy of Sciences (Azerbaijan). E-mail: antiterror-baku@mail.ru

Keywords: computer crime; detection of data; investigation.

First of all, it is necessary to determine quantity and types of servers and work stations, and the total number of computers used. In addition, network systems and computer networks used in application composition of the program should be used. The existence of the detention place must be defined, and also the backup. Special attention should be paid to the establishment of communication means for communication. At the same time, data protection and Internet access should be defined [1].

To ensure information security is necessary:

- to prevent power outages in the enterprise, to ensure the protection of the switch;
- organization of officers and other persons to ban the use of computer installations;
- all participants of the investigative action or information about the inadmissibility of use to notify existing information in computers for personal interests.

During the examination of the scene computer network, and the server should search. The limited access to the server is assigned a central server room. But apart from a local server, there are other places, central air-conditioning. Computer network that is connected to a computer through a cable from abroad is possible to determine locations. There is significant information regarding the crimes related computer network to the two destinations:

- Office building or group of buildings located within the local network (LAN) data collection;
- Administrative district located in a city or local network to collect information (companies and branch network) [3].

In both cases, where are placed all computers, the investigation group has to simultaneously view or to search the network. These types of investigations are carrying out preparatory work in advance. Access to a deleted resource can damage information on any computer. This situation reduces the effectiveness of searching and browsing the computer. Also, always a large-scale investigation required number of employees and witnesses not allowed to the amount of computer networks. From this point of view, the local network is arrested. These actions can enhance the look and feel of computer tools to monitor the events that are taking place in accordance with procedural rules. The criminal investigation was complete, objective and comprehensive investigation only in this case studies. Of course, this depends on the size and amount of information in situations such as computer disappeared from the criminal term of arrest. Even a minimum prison sentence of operational-search group, the computer to adapt to the conditions existing information on the disappearance volume allows you to assess a short, committed. Computer networks, investigation authorities or demolition expert delivery process is costly and time [2].

Thus, to ensure minimal changes, you can prevent unauthorized change in the situation of the local computer networks, computer data contained in the information resources. It should be noted that the arrest of local computer networks is practically in many countries (the Netherlands, Belgium, USA, etc.).Implementation of arrests on computer networks permitted in these countries allows for the protection of sensitive, accidentally erased or easily erased information, from poor quality control of the computer network and data carriers [4].

At present, the dependence on Azerbaijan's computer infrastructure is rising. Attacks on computer systems so far have been hackers' world-class computer viruses, yet existing cyber-threatening threats can be expanding and worrying in the future.It is difficult to maintain the safety of technology systems. If Azerbaijan's formal and informal technology infrastructure does not become safer, it can cause serious consequences in the future.

References

1. Wall D. S. The Transformation of Crime in the Information Age, 2007, Wiley, 2007, 288 p.

2. Baturin Yu.M. Problemy kompyuternogo prava [Issues of the computer law]. Moscow, 1991, 272 p.

3. Vekhov V.B. Kompyuternye prestupleniya: sposoby sovershenstvovaniya I raskrytiya [Computer crimes: ways of commissions and disclosure]. Moscow, 1996, 182 p. Krylov V.V. Informatsionnye kompyuternye prestupleniya [Informational computer crimes]. Moscow, 1997, 224 p.

4. Yakovlev A.N. Teoreticheskie i metodicheskie osnovy ekspertnogo issledovaniya dokumentov na mashinnykh magnitnykh nositelyakh informatsii [Theoretical and methodological basis of an expert examination of the documents on computer magnetic media information]. Dis…kand.yurid. nauk. [PhD in Law Dissertation]. Saratov, 2000, 218 p.