The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 09 Pages: 54-59
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

Journal Website: https://theamericanjournals.com/index.php/tajpslc

Research Article

COMPUTER-INFORMATION CRIME SCREENING TACTICS

Submission Date: September 20, 2023, Accepted Date: September 25, 2023,
Published Date: September 30, 2023 |
Crossref doi: https://doi.org/10.37547/tajpslc/Volume05Issue09-08

Imomnazarov Alisher Khasanovich
An Independent Researcher Of The Law Enforcement Academy Of The Republic Of Uzbekistan

ABSTRACT

The article explains the tactics of conducting an inspection of crimes in the field of computer information, the concept of computer-technical tools and the tools included in it, the goals and procedure of the inspection of computer facilities are described.

KEYWORDS

Review, review tactics, computer information, computer-technical tool, digital media.

INTRODUCTION

The main difficulty in investigating crimes committed using computer objects is that computer object inspection activities do not correspond to traditional inspection activities. The peculiarity of the examination of computer objects, such as programs and data, is that they cannot be examined by direct perception, they require the use of special hardware and software to access and, moreover, study them. At the same time, the investigator does not simply observe to obtain the necessary information, but enters certain commands (himself or with the help of an expert) into an automated system.

In the investigation of this group of crimes, it is necessary to interrogate different categories of citizens as witnesses: witnesses of the crime, colleagues, relatives of the suspect, computer operators; programmers, employees responsible for information security or administrators, employees engaged in technical maintenance, heads of data centers or heads of enterprises (organizations), etc.

One of the main roles of evidence in the investigation of computer crimes is the study of evidence such as computer equipment and computer data stored on it.

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 09 Pages: 54-59
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

"It should be noted that forensic literature refers to the non-traditional nature of traces of criminal activity and physical evidence encountered by the investigator in the investigation of crimes committed with the help of computers and other electronic equipment."[1] It is impossible to disagree with this opinion.

The originality of the investigation is primarily determined by the special field of crime - high technologies. "It is not without reason that in many scientific publications of recent years, computer technologies, as well as information stored in computer memory or external media (disks, floppy disks, etc.) are mentioned as a fundamentally new object of criminalistic research." This situation has a significant impact on determining the tactics of a number of investigative actions.

Let's consider a few typical cases of surveillance aimed at identifying and obtaining computer data: crime scene surveillance; inspection of the place where illegal entry was made (in case of crime by remote entry); examination of computer equipment (devices) seized during other investigative actions.

"Issues of the tactics of investigation of computer-information crimes have been considered several times in many criminological literatures"[2][3][4][5][6]. At the same time, in our opinion, some tactical aspects of its appointment and transfer should be clarified.

In the process of preparing for the implementation of these investigative actions, it is necessary to take into account the characteristics of the search objects of this category. In this regard, the investigator must follow such criminalistic recommendations, including:

- to ensure the participation of specialists in the field of computer equipment and technologies in the conduct of inspection and investigation;
- ensuring the participation of investigative and investigative bodies participating in the fight against crimes in the field of high technologies;
- giving explanations to the members of the investigative team;
- ensuring the participation of impartial people with knowledge in the field of computer technology and technology;
- preparation of necessary technical (computer) tools. "In necessary cases, it can attract expert-engineers through communication or network service." If the object of inspection is several computers (computer local network)[7], it is recommended to involve several experts in this field.

Abroad, there is a practice of actively using the help of experts in the investigation of computer crimes. For example, "Director of the United States Computer Crime Bureau Louis J. In his report to the Judiciary Committee of the US Senate, Fricks stressed the obligation to include experts in the field of computer technologies and provide them with all the necessary tools.[8] "Similar recommendations were made by other foreign experts in the fight against computer crimes.[9] "

"Yu.V. Gavrilin expressed the opinion that before starting the investigative action related to the examination of the computer equipment of the investigator, it is necessary to make sure of the specialist's qualifications."[10] This recommendation seems reasonable. In addition, to avoid such unprofessionalism, it is necessary to invite specialists who are engaged in regular computer technical expertise as experts.

The tasks of the operational officer of the unit engaged in combating crimes in the field of high technologies, included in the investigative team, are to assist the

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 09 Pages: 54-59
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

investigator in inspecting the scene of the incident, in carrying out his tasks and conducting search operations. They do the following:

- conducting surveys of citizens in order to identify witnesses, obtain other information important for identifying the criminal, search for stolen information;
- following the "hot trail" of the criminal, ensuring the preservation of the evidence and other criminalistically important information found during the inspection of the scene of the accident;
- coordination of the actions of the investigation team and other operational personnel performing the search operation at the same time.

When giving instructions to the members of the investigation team, the investigator should explain the main tasks of the future investigation, the specific features of its implementation according to the type of crime under consideration, and show the nature of each person's actions. It is also recommended to consult with an expert on the use of computer equipment at the scene of the investigation and other members of the task force.

Another important step in preparing for a computer crime scene or computer hardware investigation is to ensure the presence of impartiality. "In the literature of criminology, it is rightly noted that the impartial should have knowledge in the field of computer techniques and technologies."[11]

They can be easily found at computer service firms or among members of various clubs. It seems that the implementation of this recommendation will be an important guarantee of the reliability of the information obtained during the investigation, but in practice this does not always happen.

"In criminalistic literature, it is recommended to involve the employees working in the enterprise, organization, institution, firm, etc., as an impartial if they are not interested in the results of the work".[12]

In our opinion, the implementation of this recommendation should be approached with great care. Inspection of the scene is often carried out in conditions of uncertainty of information, as a result of which it is difficult to solve the question of interest of some employees of the organization. These individuals may include criminals, especially if they have direct access to computer data or a computer system. At the same time, since the object of inspection is valuable equipment or information, it is appropriate to inspect the incident site with the participation of the management of the enterprise, institution, organization, or firm.

Computer-technical tools that can be used in the investigation of digital crimes are, first of all, technical tools that can transmit and transport relevant data (programs or individual files). In the literature, it is called floppy disks, laser disks, high-capacity disks (for example, DVD disks, HDD, etc.) and even computers (laptops, etc.).

In addition, interesting recommendations have been developed by foreign experts in the field of combating cybercrimes regarding the examination (search) of digital devices, according to which the investigator is advised to:

- a set of targeted service programs (utilities) for computers;
- operating system floppy disks;
- virus detection programs;
- photo and video equipment for photographing the search or inspection area;

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 09 Pages: 54-59
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

- "a large amount of adhesive tape (scotch tape) for packaging, sealing of seized equipment, colored self-adhesive labels for marking confiscated items, connecting cables; paper stock for the printer, etc.[13]

A search warrant is aimed at uncovering objects that can be physical evidence in a case, and identifying and retrieving information in the electronic realm is particularly challenging.

The existence of the device environment and the impossibility of perceiving such objects in the usual way without the use of special hardware and software. In the forensic literature, there are several types of devices that can contain computer data. These include:

a) digital device used by the criminal, as well as (hidden) digital tools left by the criminal at the crime scene;

b) "transit" (communication) means that communicate with the information resources of the criminal object;

c) a digital device with illegal access.

"Information objects in digital devices do not have the same characteristics as external structure".[14] They represent not only information documents, but also traces that describe the changes that have occurred in the information field, and show the location of the necessary information.

Traces indicate the fact of finding the necessary information on a particular device or carrier. "With the modern development of technology and information technologies, criminal activity related to computer traces"[15] is spreading widely. It is necessary to take into account the guidelines for the collection of digital evidence in their activities, along with traditional trace searches by investigators and operatives.

According to T. E. Kukarnikova, a trace of a computer crime is any change in the environment (file system) related to the commission of a crime. Special information units in the file system are files, special service tables (directories, partition tables, boot records, file placement tables) and a set of clusters. change the contents of service tables (directories, partition tables, boot records, file placement tables), change the status of clusters, etc. The impact of one information object on another can be determined by the observed difference between two known states of the information object: changes in the content, format, characteristics of the file and changes in the program algorithm. "These fixed changes can be traces-mappings that describe the outcome of the interaction."[16]

Summarizing the recommendations proposed in the scientific literature for computer data crime investigations, we would like to highlight the main tactical methods that can be used and make the following conclusion:

1. Do not allow anyone (other than a specialist) to touch the computer device located at the inspection site (do not turn it on or off, do not perform any manipulations). Strangers (for example, company employees) should be removed from the scene.

2. Do not perform operations related to computer equipment or data (including copying) if the result of such actions is not known in advance.

3. During the inspection, it is necessary to determine the nature of the programs active on the computer. If a program designed to destroy computer data is running, its activity should be stopped immediately.

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 09 Pages: 54-59
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

4. "It is advisable to start the study of the situation at the inspection site by studying the nature of the computer equipment activity: whether the computers are connected to a local" or global network, the presence of additional equipment (scanners, printers, modems, streamers, etc.), whether there is information about any security devices and etc. The protocol should describe the nature of the connection between technical devices, the presence of connectors for connecting other equipment, and reflect standard technical devices. It is desirable to draw up computer equipment placement and connection schemes.

5. To provide the nature of the programs running on the computer during the inspection, the image on the screen and its detailed description in the report. It is important to reflect the results of the programs in the report.

6. Copying of the necessary information for the examination should be done on pre-prepared technical means. If such copying is not possible for technical reasons, the storage medium of the entire system unit or other device must be removed.

7. Removed items must be packed in such a way that they are not damaged. During their storage, all measures should be taken to preserve objects and information on them (for example, do not place floppy disks near a source of electromagnetic radiation, heat devices).

REFERENCES

1. Краснова Л.Б. "Обыск-осмотр" средств компьютерной техники // Воронежские криминалистические чтения. Вып. 1-Воронеж, 2000. с. 106
2. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной информации // Законность. 1999, № 3.
3. Гаврилин Ю.В. Расследование преступлений в сфере компьютерной информации. с. 81-91
4. Крылов В.В. расследование преступлений в сфере компьютерной информации. с. 242
5. Вехов Б.В. Компьютерные преступления.- М., 1996. с. 155-159
6. Кушниренко С.П., Панфилова Е.И. Уголовно - процессуальные способы изъятия компьютерной информации по делам об экономических преступлекниях.- СПб., 1998. с. 29-35
7. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной иформации // Законность. 1999, №3.
8. Statement for the record of louis J.Freeh , Director of Bureau of Investigation on Cibercrime before the senate committee on Judiciary subcommittee for the technology, terrorism and government information Washington, D.C.
9. Айков Д., Сейгер К., Фонстрох У. Компьютерные преступления.- М.,1999; BloomBecker J.J. The investigation of Computer Clime. Columbus, 1992.
10. Гаврилин Ю.В. Расследование преступлений в сфере компьютерной информации. с. 81-91
11. Комиссаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной информации // Законность. 1999, № 3.
12. Расследование неправомерного доступа к компьютерной информации./Под ред. Н.Г.Шурухнова. с. 129
13. Айков Д., Сейгер К., Фонстрох У. Компьютерные преступления.- М.,1999; BloomBecker J.J. The investigation of Computer Clime. Columbus, 1992. с. 230

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 09 Pages: 54-59
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

14. Яковлев А Н. Теоретические и методические основы экспертного исследования документов на машинных носителях информации. Дисс. канд. юрид. наук. - Саратов 2000.
15. Некоторыми учеными такие следы называются «виртуальными» (см.: Мещеряков В.А. Механизм следообразования при совершении преступлений в сфере компьютерной информации // Известия ТулГУ. Серия: «Современные проблемы законодательства России, юридических наук и правоохранительной деятельности». Вып. 3 - Тула, 200).
16. Кукарникова Т.Э. Проблема криминалистического исследования электронных документов // Известия ТулГУ. Серия: "Современные проблемы законодательства России, юридических наук и правоохранительной деятельности". Вып.3.-Тула, 2000.