Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

FEATURES OF CONDUCTING PRELIMINARY INVESTIGATIVE ACTIONS IN CRIMINAL CASES RELATED TO THE CREATION, USE AND DISTRIBUTION OF MALICIOUS PROGRAMS

Dilrabo Topildieva
Senior Lecturer, Tashkent State Law University
d.topildieva@gmail.com
ORCID: 0000-0002-8384-8183

Abstract
The article analyzes the specific features of conducting initial investigative actions in criminal cases related to the creation, use, and distribution of malicious software. It examines tactical and organizational aspects of preparing and carrying out investigative measures such as inspection, search, seizure, interrogation, and the appointment of forensic examinations, taking into account the specific nature of computer information as an object of forensic analysis.

Keywords: Malicious software; computer information; digital evidence; initial investigative actions; inspection; search and seizure; computer forensic examination; digital storage media; network topology; operational-search activities.

Introduction

In forensic literature, increasing attention is being paid to the specific features of investigative and search actions, operational-search measures in cases related to the commission of crimes in the field of computer information. They are reflected in the scientific works of V.V. Krylov, V.B. Vekhov, V.Yu. Rogozin, Y.V. Gavrilin, V. D. Kurushin, A.V. Shopin, in a number of scientific articles, in various textbooks, manuals, methodological recommendations.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

In the category of cases under consideration, inspection, search, seizure, interrogation, appointment of an expert examination, investigative experiment and other investigative actions are carried out. However, the specific features of such crimes do not predetermine individual investigative actions that are carried out more often than others.

Operational and search activities carried out by operational and operational-technical units in close cooperation with the investigator also play a significant role in solving the crime. As noted above, the majority of criminal cases are initiated and solved thanks to the activities of operational units.

As is known, the development of investigative actions is divided into a number of stages: preparation of the results of investigative actions, their direct development and detection. The main rules related to the tactics of developing individual investigative actions are described in detail in the criminalistic literature.

In cases related to the creation, use and distribution of malicious programs, the preparation of investigative actions begins with the stage of conducting an investigation and analyzing information that is important for developing specific investigative actions, understanding the tasks facing the investigation. When examining computer systems and data carriers, information about the type of data carriers, the composition, type and configuration of the hardware and technical means of computer equipment, the software installed and running on a particular computer system, the forms (formats) of file presentation on a particular machine are of great importance. Without studying this information, it is difficult for an investigator and specialist to select the necessary computer equipment that will be required to carry out the examination.

Particular attention should be paid to determining the topology of the computer network, the location of its main elements (servers, data storage devices, hubs, data input-output network devices, etc.), the possibility and availability of connections with other computer networks, including global computer networks.

Also important is information about the malware itself and its properties. If a malware capable of self-propagation is detected, in addition to the already detected copies of the malware, it may be present on other media of the victim's

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

machine, as well as in other places, for example, in areas associated with computer systems.

The location of individual elements of the computer system in the inspected (searched) room is studied, their purpose is determined, the presence and possibility of connections with other computer systems are determined. In this case, the location of jumper cables and the possibility of connecting or disconnecting certain devices from the computer system without entering the room, as well as directly in the room itself, are determined. Depending on the tasks solved during the investigative action, the investigator, with the help of specialists, must decide on the need for such a shutdown of the computer system or, conversely, ensuring the continuity of communication, which implies taking a number of measures, including protecting the most important nodes of the network. In addition to wired communication devices, mobile communication devices may also be present and used in the room, which must also be taken into account.

If computer equipment is present in several rooms during the search, it is recommended to organize a group search simultaneously in all rooms where computers are installed.[1] It is recommended to pay attention to the need to pre-check the premises for the presence of electromagnetic, magnetic and other radiation and external influences, as well as to identify their sources. In addition, the possibility of quick destruction of incriminating materials by the criminal when the investigative and operational group enters the room should be assessed. "To do this, they may use special devices designed to destroy the contents of machine storage media, as well as devices adapted for these purposes, and other objects and substances suitable for this.

In connection with the specifics of a number of material objects that must be encountered when conducting investigative actions in the category of criminal cases under consideration, it is necessary to observe certain rules for the search, registration and seizure of computer data and its devices, the main of which, in our opinion, are:

[1] Averyanova T.V., Belkin R.S., Korukhov Yu.G., Rossiyskaya E.R. Criminology. Uchebnik dlya vuzov, 1999. - S.953-954.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

- strict compliance with the requirements of criminal procedural legislation in the process of conducting investigative actions;
- compliance with the criminalistic rules for working with objects that are carriers of information of forensic significance;
- prohibition of performing any actions with the data and computer data contained in them, if the result of such actions is not known in advance and the initiation of this result contradicts the nature and procedural order of the investigative action;
- during investigative actions, the limited use or refusal to use technical and forensic tools whose working principle is based on the use of magnetic fields, electromagnetic, X-ray, ultraviolet and other radiation, as well as the restriction of tools that can damage computer data;
- be careful when working with powders and chemical reagents used to identify and correct traces and foreign layers, preventing their entry into the working surfaces of machine information carriers, connectors, devices working with removable machine information carriers, etc.;
- use special terminology when recording the operation and characteristics of computer systems and computer data;
- when examining computer data, the rules for examination and description must be observed, from general to specific, from directories to individual files, from general characteristics of file properties to its specific composition;
- identification of the appearance of computer system elements, machine storage media and the content of computer data must be carried out in as much detail as possible, observing the rule of relativity of information to the crime under investigation;
- use certified software and hardware during the examination of computer equipment;
- only computer equipment that contains or may contain information of forensic significance should be seized.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

The result of the preparatory stage is the development of a plan for conducting investigative actions. However, the preparatory stage of investigative actions does not end there. It can be continued directly at the place of their conduct.[2]

The examination of the investigative action is carried out in accordance with the requirements of criminal procedural legislation and general tactical recommendations. The problems of its conduct are covered in detail in the criminalistic literature. Also, examination is the process of cognition of the activity based on the sensory perception of the object of research, the subsequent understanding of the identified facts, the establishment and assessment of the connections between them.

Examination of cases related to the creation, use and distribution of malicious programs is associated with a large amount of use of special knowledge in the process of its implementation, special technical means that allow checking computer data, etc.

During the investigative action, the use of computer technology should be prohibited for all persons not related to the investigative actions being carried out. All manipulations with computer equipment should be carried out by the investigator or another person or specialist conducting the inspection.

In the literature, descriptions of investigative actions for crimes in the field of computer information are given mainly in the form of algorithms of actions and, of course, their positive role is revealed[3]. The methodological recommendations for the examination, strengthening and seizure of computer equipment prepared in the course of this study include the main features of the examination of computer equipment. However, the examination of computer equipment is incomplete without examining computer data located on machine media. The features of such an examination are reflected in the methodological

[2] For more information on direct action at the location of the investigative action, see! For example: Katkov S.A., Sobetsky I.V., Fedorov A.L. Podgotovka i naznachenie programmno-teknicheskoy ekspertsiy / Bulletin GSU MVD USSR, No. 4, 1995; Averyanova T.V., Belkin R.S, Korukhov Yu.G., Rossiyskaya E.R. Criminology. Uchebnik dlya vuzov. 1999. - S.953-954; Criminalistics: Uchebnik dlya vuzov/ Pod ed. prof. A.F. Volshskogo, 1999. - S.597-598 and others.

[3]Andreev B.V., Pak P.N., Horst V.P. Investigation of crime and computer information. - M.: OOO Izdatelstvo "Yurlitinform", 2001. - P.51-63 i drugie.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

recommendations for the examination of computer data located on machine media.[4]

After the detailed examination is completed, an expert examination is scheduled to determine all further actions with the information carrier, including the resolution of problems that arose during the examination.

Also, during the search and seizure, special attention should be paid to recording the state of the criminal's computer system, the introduction of malicious software and the consequences of the impact, as well as the seizure of information and documents from the devices indicating the preparation and commission of this or other crimes (algorithms recorded on paper, source codes of programs, descriptions of some programs), computer systems, user data, access passwords, etc.).

In most cases, when searching for cases of the category under consideration, as in the main part of other criminal cases, special attention should be paid to searching for possible caches. At the same time, the use of a particular search engine should be very limited, since its impact can damage information stored on machine tools.

In the investigation of crimes of the category under consideration, interrogations are carried out more often than in the investigation of other crimes.

In the preparation and conduct of interrogations, as in other investigative actions, a specialist in the field of computer technology can provide great assistance. For example, he can explain incomprehensible technical points to the investigator, determine the sequence of technical questions and the level of their concretization.

References:

1. Averyanova T.V., Belkin R.S., Korukhov Yu.G., Rossiyskaya E.R. Criminology. Uchebnik dlya vuzov, 1999. - S.953-954.
2. For more information on direct action at the location of the investigative action, see! For example: Katkov S.A., Sobetsky I.V., Fedorov A.L. Podgotovka i naznachenie programmno-teknicheskoy ekspertsiy / Bulletin

[4] Methodological recommendations for inspection, fixing and inspection of computer technical equipment.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

GSU MVD USSR, No. 4, 1995; Averyanova T.V., Belkin R.S, Korukhov Yu.G., Rossiyskaya E.R. Criminology. Uchebnik dlya vuzov. 1999. - S.953-954; Criminalistics: Uchebnik dlya vuzov/ Pod ed. prof. A.F. Volshskogo, 1999. - S.597-598 and others.

3. Andreev B.V., Pak P.N., Horst V.P. Investigation of crime and computer information. - M.: OOO Izdatelstvo "Yurlitinform", 2001. - P.51-63 & others.
4. Methodological recommendations for inspection, fixing and inspection of computer technical equipment.