UDK 343.98:004.056.53

INSPECTION OF THE SCENE DURING THE INVESTIGATION OF COMPUTER CRIMES

H.I. DUDA, *assistant,*
Department of Theory and History of State and Law,
National University Life and Environmental Sciences of Ukraine

This paper describes one of the forensic issues, such as viewing the scene. This issue is important for law enforcement authorities in the investigation of crimes in the sphere of computer systems and computer networks. It is one of the most informative actions during the investigation of computer crimes.
Computer, crime, investigator review, computer information, investigations, Criminalistics.

Inspection of the scene allows you to explore a number of important conditions such as the nature of the event and signs of traces of the crime; the place where the crime was committed; who was involved; which are distinctive features of action of each of the participants in this event; motives and purpose of their actions; tools, objects that were left at the scene. We can explore the facilities and documents used to access the object assault and committing legal actions with them; who could observe this event; aspects that lead to harmful consequences, such as criminal acts of officials.

The purposes of the article review the concept of investigator review, as well as analysis of spot observations during the investigation of computer crimes.

There are many definitions of investigative review in the literature. Thus, Yakymov noted that the investigator review is the actions aimed at establishing the material data that are relevant to solving crimes and identification of perpetrators.

According to Kubiczkij, the review is a detection of physical attributes of the objects. On the other hand, Strogovich called it as a procedural action that aims to identify, fixation and investigation of the characteristics and conditions of different subjects establish the circumstances which are important in case. However, this definition is formulated in an insufficient measure that distinguishes it from other investigations, whose task is also to identify and fix attributes and classes of objects.

In our view, the concept of investigative review was most fully and correctly interpreted by Kolmakov. According to Kolmakov, the investigator review should be understood as an investigative procedural action in which he finds accepts, examines, evaluates and fixes of the quality and characteristics of the material objects that are associated with the

investigation of the events in order to identify circumstances that have values in establishing the truth of the case.

The task of the investigator consists in collecting evidence. The investigator makes versions of the nature of the investigation of computer crime and its members, the location of objects that have probative value, the effects of crime, etc. based on the available evidence.

Law enforcement officials are faced with the need for review of computer technology, including various storage devices during certain investigations. The main problem that arises in the course of the investigation is that the subject cannot directly examine the structure of storage media because it is a magnetized area of magnetic media. To solve this problem, you need to use some intermediate element that allows the subject, which carries out a review, comprehensively and objectively evaluate the information on storage media. Therefore, the question of software used in the course of some investigations is extremely important.

According to Dulov, place of incident is the plot areas, underground facilities, natural formation or premises in which there was a criminal act or detected its consequences such as material traces that have spatial, temporal and causal connection; it is an territory where there was an act.

The problem of inspection of the scene in the investigation of computer crimes are devoted the works by Kozlov, Vyehova, Popov, Ilyushin, Andreev and other authors.

The question of the inspection of the scene in the investigation of computer crimes is often reported in the forensic literature. Thus, Krylov said that investigator should have a set of service programs during the investigation, providing methods for determining the quality of a computer; check some external storage devices; work with files; tool to find hidden information. Selection of these programs is based on own experience of the investigator.

The investigator may encounter any technical difficulties, despite his knowledge and experience. Instruments of crime can be investigated by special software.

Standard software is not always possible to solve the problem of determining the inspection scene in different situations. When we examine a crime, for example, the illegal access to computer information, we can have a few places where the event occurred:

- the workplace is a place of information processing, which has been the subject of a criminal assault;
- the place of storage or backup information;
- the place of use of technical means for unauthorized access to computer information held elsewhere. This place can coincide with the workplace;
- the place of preparation for a crime such as the development of viruses, hacking, password selection or place the direct use of information

obtained as a result of unauthorized access to information stored on storage media or a computer.

The scene can be one premise where installed computer and stored information or number of premises including various buildings located in different territories or part of the territory, where is held the remote solenoid or audio interception.

It is necessary to take measures to protect the place of incident and provide safety information on computers and peripheral storage devices after the arrival investigative team to the scene.

It is necessary to invite specialists in computer technologies such as programmer, systems analyst, engineer or maintenance of a communications network to improve the efficiency of the inspection scene. Professional Profile is determined according to the investigation of the situation, goals, objectives, investigative actions, and computer hardware and installed software. We invite other persons who understood in computer technology and can help in the investigation the scene. We invite other persons who know computers and can assist in the investigation of the place of incident. We need to resolve the issue of material and technical support while preparing for the examination. The investigator and expert can apply traditional techniques and forensic detection and special equipment such as special software for accessing, reading, and storage of the computer media.

The experts examine individual computers that are not connected to the network; workstations that are included in the network; servers and telecommunication devices and magnetic data carriers; technical and other documentation, as well as premises in which the equipment is located.

It is advisable to use the tactic "from the center - to the periphery" during the inspection of the scene. It means that the movement is carried out in a spiral on the territory, and this technique is called as "eccentric" in the forensic literature.

The investigator should examine and describe in the following order in the protocol having arrived on the crime scene:
- Computer equipment;
- Software. Particular attention should be paid to the so-called logo files (logs of programs), which can store important information;
- Floppy disks and other storage media;
- All documentation discovered at the crime scene.

The inspector will examine and record all the protocol, and then the protocol need to pack and seal. It should be to label both ends of the cables during disassembling equipment. In addition, experts do photos of general view premises and compose its plan, which shows the location of the equipment and mutual connection. If your computer is connected to the telephone network, you should determine whether your computer is connected via a modem. If it is a phone jack, you should turn it off. If it is

connected via a modem, the voltage of the device is switched off and recorded the phone number in the protocol used while connecting.

Then, monitor and CPU are turned off and disconnected voltage. Location PC and its peripheral devices carefully recorded in the protocol of investigative action and application diagram. Describes the procedure of interconnect these devices, indicating the features of connecting wires and cables; before disconnection is useful to make a video or photograph the junction.

The processor is packaged in sealed special membranes that provide reliable transportation. Portable computers, diskettes, separately mounted hard drives, storage media that can be used with your computer (tapes, floppy disks, CDs, flash cards, etc.) are packed in individual sealed bags and boxes. Equipment should be ambient temperature during packaging. All items and documents should be extracted and described in accordance with the current criminal procedure law.

Overview of computer technology and information extraction is carried out in the presence of witnesses. Witnesses should have the necessary knowledge in computer technology. If the witness is incompetent in this area, he cannot convince the recognition of certain circumstances in court.

Results of the survey of investigators and employees of the Interior indicate that the majority of respondents could not identify a specific spot observations in cases of computer crime.

According to Gross, viewing the scene is the cornerstone for becoming a forensic and remains relevant to this category of cases. The specificity of this type of review is determined by the investigator, who should immediately investigate the place where the tracks and other evidence were found at the place of computer crime. This information is the basis for building a version that is grounded propositions about the incident and persons related to it.

According to the survey areas, investigating computer crimes has a number of circumstances that contribute to inspection areas and premises and fall under the traditional understanding of the scene. It is a building, telephone lines, office automatic telephone exchanges, cable management, other network equipment, etc. The crime scene as opposed to place of incident is the region where the offense was committed or is offensive elements of the criminal consequences that could be present in another area.