Improving the algorithm of organization and tactics in conducting separate investigative actions in the field of ecology

Evgeniy Nazarkin[1], *Talat* Suleymanov[1], *Yuri* Truntsevsky[2,*], and *Roman* Osokin[3]

[1]Academy of the Federal penitentiary service of Russian Federation, 1 Sennaya str., Ryazan, 390000, Russian Federation
[2]Institute of Legislation and Comparative Law under the Government of the Russian Federation, Cheremushkinskaya str., 34, Moscow, 117218, Russia
[3]Bauman Moscow State Technical University, Baumanskaya 2 str., 5/1, Moscow, 105005, Russia

Abstract. Studying the elements of organization algorithm and tactics in conducting separate investigative actions during crime detection in the computer information area, such as incident site inspection, assigning criminalistic expertise and using the records of the criminalistic registration system of the Ministry of Internal Affairs of Russia. In the process of studying the problem under consideration, the following general and particular methods of scientific cognition of real and objective reality were used: dialectical, logical-legal, statistical, system analysis and specific socio-professional research methods. The authors analyzed, summarized and synthesized the problems in preparing and conducting inspection of the incident site in cases of crimes committed using computer technologies. Characteristic features, main directions and possibilities to identify traces during the inspection, and, accordingly, the purpose based on the inspection results and other investigative actions, certain recommended types of court expertise were examined. Study of possibilities to use record keeping arrays of the criminalistic registration system of the Ministry of Internal Affairs of Russia in the course of work with traces and objects obtained was carried out. The authors studied the problems of organization and tactics in conducting investigatory inspection, appointment of court expertise, using the records of the criminalistic registration system of the Ministry of Internal Affairs of Russia in the course of investigating crimes in the computer information area; ways were suggested to improve preparation and conduct these actions indicating the elements that increase efficiency of this investigation algorithm in the considered category of crimes.

1 Introduction

Many specialists and experts in jurisprudence, in particular criminologists and criminalists, note that in recent years the number of cybercrimes is steadily increasing. This is connected to daily Internet use, availability and popularity of digital technologies,

*Corresponding author: truzev@yandex.ru

increasing cyberspace in general, computerization of public and private structures, transfer of paperwork, money and commodities circulation of citizens and society to the computer information circulation. Accordingly, the number of people trying to get rich through the use of computers, telecommunication systems, knowledge of the features of programming and communication in the world computer systems is increasing. At the same time, level of intellectual knowledge of criminals is increasing, and even, like some modern feature, their age threshold is lowering, which allows them to adapt to new modern technologies and successfully commit crimes using communication tools.

Criminologists in information and telecommunication technologies note that cybercrime detection is characterized by a steady downward trend, given high latency, generality and accessibility for the majority of the population. In our opinion, this is objectively connected not only to factors and problems listed above, but also to the fact that the law enforcement system of Russia is not preparing the corresponding highly professional personnel to fight against these crimes. It means that there is a trend, request from society and the country law enforcement system, but the existing implementation of the program to effectively combat these types of crimes is unable to be realized. For example, the number of crimes in information and telecommunication area increased by 37% from 65,949 in 2016 to 90,587 in 2017. Moreover, the share of these crimes to the number of all crimes registered in the Russian Federation is slightly more than 4%, i.e. this is almost every 20th registered crime. While the real estimated share of latency is dozen times higher. Number of cybercriminals hacking into various platforms, systems, accounts of institutions, organizations and individuals is increasing.

The list of crimes related to computer technologies was legally and juridically expanded: fraud using electronic means of payment (Article 159.3 of the Criminal Code of the Russian Federation); crimes in the computer information area (Chapter 28 of the Criminal Code of the Russian Federation); illegitimate access to computer information (Article 272 of the Criminal Code of the Russian Federation) ; creation, use and distribution of malicious computer programs (Article 273 of the Criminal Code of the Russian Federation); violation of the rules for operation of means of storage, processing or transmission of computer information and information-telecommunication networks (Article 274 of the Criminal Code of the Russian Federation). And although a downward trend is observed in some criminal components, this is primarily due not to unpopularity of these methods of crime with criminals, but to the possibility of the latter passing to more “advanced” technological, quick and safe methods of committing crimes for them based on modern improving products in information-telecommunication systems of information access and exchange.

As follows from the statistical surveys of the General Prosecutor’s Office and the Ministry of Internal Affairs, the most popular cybercrimes today include illegitimate access to computer information (Article 272 of the Criminal Code of the Russian Federation), dissemination of malicious computer programs (Article 273 of the Criminal Code of the Russian Federation), as well as fraudulent actions committed with electronic means of payment (Article 159.3 of the Criminal Code of the Russian Federation). It should be noted that access to confidential information or information constituting state secret by a person, who does not have the required authority (without the owner or his legal representative consent) is considered illegitimate provided that special means of information protection are installed.

The share of undetected crimes, or the so-called negative detection of cybercrimes, is increasing. Thus, 903 crimes were investigated in 2017, the number of undetected crimes was 790 (the so-called remainder). In 2018, 726 crimes were investigated, and the remainder of undetected crimes was 1,031 [1, p.3]1. All this indicates the increasing demand of the state and society for the country law enforcement system ability to fight such

crimes, which, in turn, determines the relevance and the object of the topic of research on this issue.

2 Methods

Literary sources on this problem and archival materials of 18 criminal cases related to the investigation of illegitimate access to computer information in the Ryazan and Moscow Regions for the 2002-2017 period were studied. Discussion materials were used of the V All-Russian scientific-practical conference "Criminal Procedure and Criminology: Theory, Practice, Didactics (Modern problems of pre-trial proceedings: criminal procedural, criminalistic and organizational aspects)" (Ryazan, December 6, 2019).

In the process of studying the problem under consideration, the following general and particular methods of scientific cognition of real and objective reality were used: dialectical, logical legal, statistical, system analysis, concrete sociological and professional research methods.

The problems associated with solving and investigating crimes in the computer technology area, organization and tactics of certain investigative actions and special investigation activities were addressed by well-known criminalist scientists and criminologists such as Ali M.N. [11, p. 1], Kravets Evgeniy, Steshenko Yulija, Likholetov Aleksandr, Daniyar V., Kairgaliev, Vasiliev D.V. [2, p. 585], Hertley Timon [3, p. 6], Aratuly Kuanysh, Baigazy Yerlen, Tarap Zhazyra [4, p. 111], Christopher Rigano [5], Vekhov V.B. [12, 13, 14. 15, 16].

3 Results

If we consider the tactical tools of crime investigation authorities, it is envisaged to improve the tactical actions algorithm for successful investigation of the given crimes in addition to the usual evidence (direct and indirect), such as various protocols of investigative actions, operation, information and referral measures, various types of checking records of the criminalistic registration system of the Ministry of Internal Affairs of Russia aimed at identifying criminals, criminal relations, circumstances of a crime, collecting evidence of a person guilt and innocence, establishing consequences of a crime and elimination thereof, as well as proposed preventive measures.

Law enforcement agencies are using various legitimate means in proving a person guilt or innocence, such as conducting separate investigative actions (inspecting the incident site; investigative inspection of objects and documents that could serve as material evidence; certification; personal and premises search; interrogating suspect, accused, witness and victim; appointment of a court expertise; investigative experiment and evidence verification on site, identification, control and registering negotiations, etc.). In addition, investigation authorities are taking information from the organization, where the "leak" of information occurred or any other criminal consequences were identified.

When considering the tactics of conducting separate investigative actions as the direct working tool of an investigator, the role of inspecting the incident site should be immediately noted. Analysis of the 18 archived criminal cases related to investigation of the illegitimate access to computer information in the Ryazan and Moscow Regions in 2002-2007 demonstrated the fact that this investigative action, despite its originality and urgency, was not always the first one; however, its execution in this category of crimes is always required.

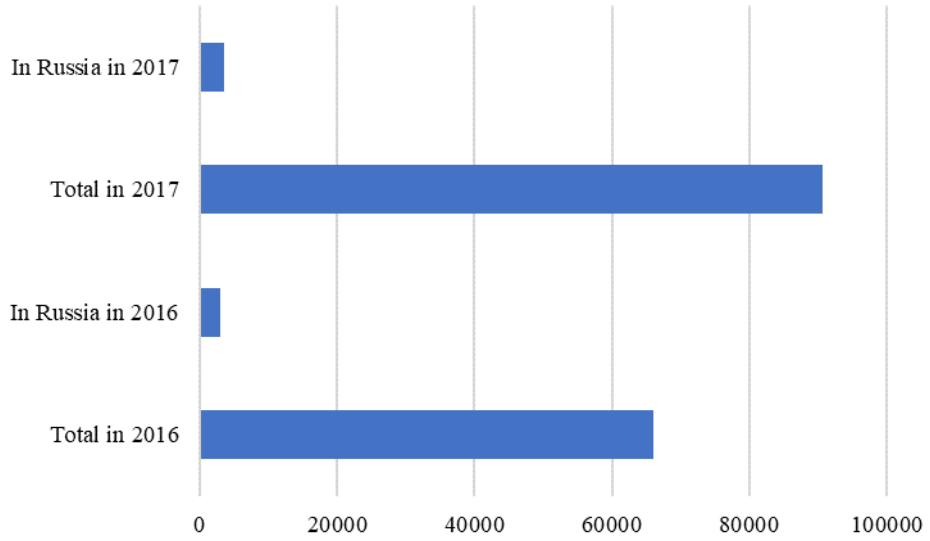

Fig. 1. Number of crimes in the field of information and telecommunications.

This fact algorithm is connected to the crime specificity, which first determines obtaining sufficiently detailed information about it, for example, through a survey (detailed explanation) of the applicant (victim, who, in turn, could be working in the network on the basis of an agreement with the provider company), clarification of the harm caused (material damage amount), method of the crime, time of committing it, possibly the persons involved (interested) in it and other circumstances.

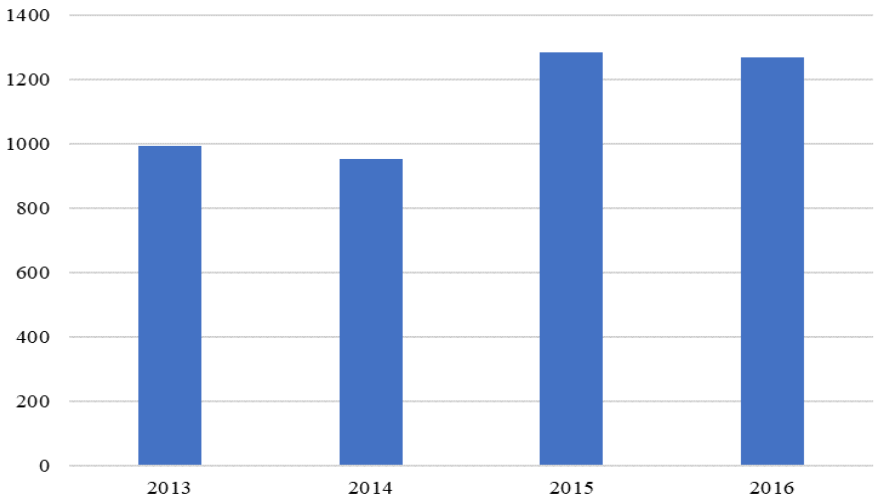

Fig. 2. Dynamics of the average amount of damage from information leaks, million rubles.

All these circumstances are started to be clarified by the investigator during the interview in the course of receiving statement of a crime with possible involvement of specialists in the high-tech area (usually, engineers in computer and telecommunication technologies) and operation staff of special units of the Ministry of Internal Affairs to combat this category of crimes [1].

Studying peculiarities in tactics of the incident site inspection in cases of this category, it should be noted that preparation for an investigative action before the deployment of the investigative operation group includes the following actions:

− probable coordination of place and time of the incident site inspection with interested parties (applicant-victim, provider representative), on the one hand, as well as duty service and operations department, on the other;

− selecting and ensuring participation of specialists, who could provide significant assistance during the incident site inspection of computer equipment, networks, information on various media, documentation connected to working in the information system on a specific computer;

− ensuring involvement of witnesses of the investigative actions, i.e. persons not interested by law, to carry out investigative actions;

− preparation for use of video and scanning computer equipment that would assist in inspecting, registering and saving the discovered evidence;

− organizing and conducting a detailed briefing of members of the investigative operation group with preliminary separation of their duties during the proposed inspection period, highlighting certain peculiarities in handling computer equipment, as well as the criteria for general behavior of officers participating in the inspection;

− in some cases, when the inspection objects are allegedly known, conducting preliminary oral consultations with specialists participating in the investigative activities [1].

It should be noted that video and scanning equipment scanning a computer (for example, duplicators for copying information from the computer being inspected) used in the incident site inspection is usually available with appropriate specialists or with an investigator specializing in crimes of this type.

The role of such specialists, including, as a rule, programmers is significantly increasing at present. This is objectively connected to specific circumstances.

Computer training of investigators still remains at the user level, despite continuous improvement in the cognition process of programming features, movement of electronic information, expanding capabilities of computer technology and communication means [1].

Investigator is physically unable to track new technological changes in computer systems and telecommunications, since the process of their improvement is being constantly technologically developed; moreover, it requires certain software and engineering training from the investigator.

Computer technologies experts during the incident site inspection often limited to inspecting computers, information on them, documentation, network system (including servers) are mainly carrying out actions related to specific manipulations on computers. They include: on (start) - off (exit); entry into current and potential programs that are used on this computer; establishing the latest data used by the user (suspect) with their analysis, interpretation by a specialist to the investigator; copying them as the evidence base of the investigation; detection of specific informational traces of a crime; assistance in the protocol description to the investigator of computer system, peripheral equipment, actions (operations) of the suspect; actions aimed at saving the available computer information on the inspection object ensuring prevention of its intentional destruction or damage; actual seizure of computer information, etc.

Selection of a concrete specialist remains with the investigator based on specific tasks of inspecting the incident site, type of crime, suspect personality and algorithmic stage of covering the investigation element as a whole. Thus, in the course of executing the investigative task of identifying information on a computer or actions (manipulations) of a suspect with it, as well as outside attempt to use, harm or steal it, a specialist programmer is required, who knows the basics of computer systems software, organization of computing

and telecommunication processes, methods and means of information protection and information security.

To solve the investigation task of inspecting and impounding the computer technology technical means, a specialist understanding elements and devices of computer technology, its control systems, communication systems and information flows (technical engineer, electronic engineer, for example) would be useful.

Coordination of the incident inspection place and time with the interested parties (applicant-victim, provider representative), as well as with members of the investigative operation group and duty service requires the investigator to take organization and management decisions. If possible, it is necessary to coordinate in advance the incident site inspection time and place taking into account the urgency of such inspection and its effectiveness, which much more depends on the group composition, its equipping with special technical, criminalistic and computer means for reading, copying and saving information that was found and seized.

Preliminary consultations on these issues are usually carried out with all participants of the upcoming inspection by telephone with the expanded range of its features. In our opinion, the investigator should foresee possible extension in the inspection tasks based on type of crime, alleged criminal personality and inspection object. Besides, such investigator should also consult a specialist about the possible technical means involved in the effective inspection.

When organizing attraction of witnesses of an investigative action, i.e. people not involved by law, to carry out investigative actions, the investigator should take into account, in our opinion, first of all, the incident site and object of inspection. Thus, when the investigative operation group arrives at the incident site, as the criminalistic guidelines recommend, the investigator should try to entrust the search for and participation of witnesses of investigative action to the operation officer, who may appear secretly at the site even before arrival of the main group, or to the local police officer, if his participation would be rational in a particular situation.

If this was not done in advance, then the investigator upon arrival at the incident site possibly selects witnesses from among those not uninterested in the criminal case, who should generally outline the essence of such inspection; and it is also advisable to obtain initial (user) data on computer equipment.

In case a computer is inspected that is located in residential premises, it is recommended to invite neighbors, i.e. young and middle-aged people, as a rule, understanding computer technology as users.

If the inspection is carried out in organization or institution, then naturally their representatives, employees or even visitors are invited as witnesses; the status of a witness in the investigative action in this case is also not violated. Local police officer on the territory, as a rule, is not involved in organizing the inspection. Main condition for selecting such a witness for inspection both in the organization, as well as in the living premises, is disinterest in the outcome of a case. Given confidentiality, expensive equipment and software, it is advisable to conduct an inspection with participation of enterprise, institution, organization or private company management, as well as of its materially responsible persons.

For effective inspection of the incident site and taking into consideration the inspection technical nature, the investigator prepares video and scanning computer equipment assisting in inspection, registration and saving the evidence information discovered in this case, including traces of the crime. As a rule, the investigator takes with him a laptop with large memory and fast operating system, various cables for connecting additional copying and scanning equipment, special computer programs that allow copying and quick analysis of

the information being examined at the incident site. For insurance, the investigator takes with him a hard drive with large memory capacity.

During the briefing of participants to the investigative operation group with distribution of their duties during the inspection, particulars of handling computer equipment and behavior of all those present during personal examination, the investigator draws attention to secret monitoring of persons present during the inspection.

Computer equipment and its software are quite expensive equipment that requires accurate and competent handling. In addition, it is someone's property. It is better to entrust its handling to a computer systems specialist participating in the incident site inspection. It is recommended that other inspection participants perform any physical action or manipulation with computers and components only with permission of the investigator and specialist.

During the next phase of the incident site inspection preparatory stage and upon arrival of the investigative operation group at the inspection site, it is recommended to conduct a general visual inspection to establish features of the upcoming inspection, its key nodes, presence of certain persons (probable suspects or witnesses), current equipment mode of connecting the equipment. In addition, orientation and overview registration of the inspection site situation on photo and video equipment is provided. Investigator based on actual orientation at the inspection site organizes protection and inviolability of the equipment being inspected before the involved specialist starts working with it.

Before starting the inspection, attention should be paid to connection of the inspected equipment to the local network, cables, circuit breakers and controls, other means of communication and commutation located in the premise or in the adjoining premises. This is due to an alleged possibility to remotely affect the inspected computer equipment, transmit information to possible accomplices and destroy information or traces of a crime. Consultations and actions of specialists involved are guiding. In addition, presence of computer connected switched systems is identified, such as teletype, telephone and fax, which should also be taken under control during the upcoming inspection.

When the computer is being switched on, or is already operating, as well as being in the standby mode, specialist and investigator determine in what software the equipment being inspected works and register this in the investigative action protocol. It is advisable to save the operating computer current state, while identifying all the previous actions of a person, who previously worked on it. In our opinion, scanning and copying tools used by specialist or investigator are introduced in this case without any preconditions and ensuring mandatory use of elementary photo and video shooting of the monitor screen.

During the so-called site inspection working stage, each object of research, each node and channel (cable with connection elements) is being carefully registered in the investigative action protocol, first, without touching them (static stage), and then, if necessary, after meaningful specialist manipulations; what is found, is the so-called dynamic inspection stage.

Specialist examines the files with text and graphic information noting their condition and damage; at the same time, attempts are made to restore deleted or eliminated files.

During the computer location (so-called workplace) inspection, it should be not missed to inspect environment, condition of adjacent surfaces and location of windows, doors, locks, premise signaling equipment imposed by trying to find trace evidence (fingerprint, DNA and smell positive sweet and fat components) and material traces (traces from tools, legs, clothes, blood, skin, etc.).

Particular attention should be paid to finding traces on the keyboard, mouse and computer surfaces. Special technical means of identifying a personal computer user are introduced quite effectively and include electronic cards, activator keys (PC access) with memory microprocessor, fingerprint identifiers (for example, Calspan), etc.

Inspection protocol, as well as the annexes to it in the form of photo-video registration (photo table, video recording), printout or duplicate of information, identifies the examined configuration of computer equipment: batched processor type, its used software version, RAM (hard drive), information about person responsible for use, etc. This information is taken, as a rule, from the Properties menu of the System working folder. Subsequently, current state of the reflected information should be preserved with registered results on the committed crime, its criminal consequences; for example: blocking the operation program, data destruction, copying or transferring information, disruption of the PC operation, its system or the network in general, to which it is connected. Thus, the method of committing a crime is established. Personal computer always as a software device registers its actions in files and this could be identified.

If during the incident site inspection there arises a possibility to seize the computer or its separate components, then this action is carried out according to the general criminalistic rules of seizure with possibility of packing and preserving available traces on the surface of objects and information stored in the device. The following actions are conducted simultaneously: interview of testimonies and personnel of institution or organization, where user netnames and their input passwords are identified; documents on computer and peripheral equipment passports are examined, regulatory documents on the PC operation, job descriptions in charge of them, personal data of users, etc. are being studied. Computer equipment is seized only after turning it off and disconnecting from the network.

4 Discussion

If it is impossible to seize computer equipment for study and, probably, for court expertise, then, as a rule, the following actions are carried out to minimize the crime consequences, while preserving the evidentiary base. These include: closing and sealing the premises with computers; shutdown of power supplies with sealing all necessary units and components; duplicators and portable hard drives are used to copy and save information about the program, files and actions from the inspected computer.

Major role as a potential source of evidence or means of proof in crimes of this type is played by such a special investigative action as court expertise usually assigned after the incident site inspection described above. Depending on the type of traces that could be left by a criminal (criminals) on the incident site and connected to computer equipment, its communication facilities and premises (where it is located or adjacent to), the following types of court expertise could be assigned:

- court computer technical expertise (CCTE);
- court telematic expertise;
- court fingerprint and poroscopic (ejectoscopic) expertise;
- court trasological expertise of footprints (shoes);
- court trasological (mechanoscopic) expertise of hacking tools and instruments, production mechanisms of their traces;
- trasological expertise to establish the whole by parts;
- trasological expertise of locks, locking mechanisms and signaling devices;
- author originating expertise on any reflected medium;
- linguistic expertise using written and oral texts;
- graphic and other types of the handwriting court expertise;
- technical and criminalistic expertise of seized documents;
- phonoscopic expertise of magnetic information carriers;
- expertise of articles and objects of fibrous nature (CEMSP);
- court expertise of perfumes and cosmetic substances;
- court electrical expertise;

- court medical expertise of material evidence of biological origin (blood, saliva, sweat, hair, skin);
- medical molecular genetic expertise of discovered evidence of the biological origin;
- biological expertise of seized traces of human odor (court biological olfactory expertise) [1].

The above list of court expertise is not exhaustive, since it is possible to identify also another traces of crime and the criminal at the incident site, and accordingly, appointment and conduct of other court expertise on them.

As a rule, one of the main mandatory court expertise in this category of cases is the court computer technical expertise (CCTE). Actually, this type of expertise based on the study object and established facts and events is divided into the following subtypes:

1)hardware computer court expertise;
2)software computer court expertise;
3)information computer court expertise (data);
4)computer network court expertise [1].

Hardware computer court expertise could be carried out in order to study the computer under examination hardware unit components, as well as configuration of devices connected to it. The subject of computer technical court expertise includes all sorts of facts and circumstances that could be established in the process of studying patterns and characteristics of computer systems operation and separate computers, their units, modules and systems with various information carriers on the crime and its participants.

As a rule, objects under study of the above-mentioned computer technical court expertise subtype include: a) versatile computer systems: basic desktop (stationary) computers; portable laptops, such as notebooks; b) peripheral devices providing connection: scanners, faxes, printers, etc.; c) network hardware (servers, workstations, active equipment, network cables, etc.); d) computer conjugated systems (organizers); pagers e) mobile phones, teletypes, modems, etc.; f) component units and systems based on microprocessor controllers (transponders, immobilizers, cruise controllers, etc.); g) various sets: expansion cards; hardware units; microcircuits, including random access memory and plug-in (hard drives, “drums”), laser and magnetic disks; optical magnetic disks; flash cards, etc.

Software and computer expertise subject of research is the laws of development (creation) and application (use) of software installed on a computer in this criminal case.

Actually, the purpose of court software and computer expertise is to study functional intended use of a computer program, its characteristics and implemented requirements, algorithm and structural features laid down in it, as well as the current state of the computer system software submitted for expertise and probable intentional or careless software errors.

Objects of software and computer expertise include: a) system software (operating systems); b) accessory programs - utilities; c) development and debugging tools; d) service system information; e) application software (general purpose applications, i.e. text and graphic editors, database management systems, spreadsheets, presentation editors, etc.; special purpose applications for solving problems in specific areas of science, technology, economics, etc.) [1].

Subject of information and computer court expertise could be a general database (information) stored and operated in computer equipment (system unit) submitted to examination. The main goal of information and computer court expertise could include detection, analysis and evaluation of data (information) prepared by the user on the computer; establishment of the functional program (application software) for carrying out information processes in this computer system.

Objects of information and computer court expertise (information, data) are: files, folders, graphic images, etc. that are prepared using the above-mentioned software tools installed by the network operator with technical capabilities of expanding text formats (.txt, .doc ...), database formats (.dbf, .mdb ...), graphic formats (.bmp, .jpg, .tif, .cdr ...), spreadsheets and graphs (.xls, .cal ...); means of protection against unauthorized access; means of cryptographic information protection, data transmission system, service program, etc.

The fourth subtype of court computer technical expertise, i.e. court computer and network expertise, is substantively connected to the functional use of computers submitted for examination, which implement a certain network information technology, as a rule, expanded or limited in regard to users and information capabilities. Existing Internet technologies make it possible to connect different computers and other network equipment together in the network systems, use information about them and carry out all involved information operations (programs) and resources [1].

Objects of this CCTE subtype could include: computer and its software characteristics and properties; characteristics and properties of the Internet provider computer network (information infrastructure) and software services provided, for example: e-mail, www.-servers; structure, configuration, installed network components, capabilities and fact of access to network information and to specific computer; typical parameters of a specific class of network technology tools; tool belonging to the application server or client side; actual state and serviceability of the network tool, presence of physical defects, state of the system log, access control components; computer network initial state as a whole and of each network tool separately, place of purchase (acquisition); alterations in the initial configuration; reasons for changing the computer network properties; violation of network operation modes and facts (traces) of using external, including the “alien” hacker programs, etc.

Given the rapid improvement and further development of telecommunications and digital capabilities in cellular communications, let us distinguish emergence and introduction into practices of investigating crimes using computer technology such type of court expertise as telematics. Subject of telematic expertise could include facts established on the basis of applying special knowledge in examination of telecommunications and mobile (cellular) communications, as a technical source of material carriers of data about a crime, its participants and circumstances of its preparation, commission and concealment.

Considering the performance of separate investigative actions in the process of investigating crimes in the computer information area, it is impossible not to note such a problematic issue in the algorithm of actions based on the results of conduct, including the mentioned incident site inspection, as the possible use of information provided by the criminalistic registration system of the Ministry of Internal Affairs of Russia, as a rule, in the course of investigating the initial stage in regard to unauthorized access to computer information.

According to results of the incident site inspection, identification of the crime specific traces and persons involved in it, as well as of the technological method of commission (criminal handwriting), investigative leads are put forward. Leads are related to the event as a whole and to its separate circumstances and elements, i.e. method of committing the crime, identity of the criminal, motive, traces of the crime, possible witnesses and accomplices, time, site of the commission, size and type of damage caused, identity of the victim or legal entity, etc.

Study of these leads and, accordingly, information about the crime elements in them makes it possible to introduce and use various records of the criminalistic registration system of the Ministry of Internal Affairs of Russia, which provides the opportunity to

clarify and sometimes establish facts and information enabling to successfully conduct further investigation.

It should be remembered that these facts and information could be obtained based on their location from the Main Information Center (MIC) of the Ministry of Internal Affairs of Russia, information centers of the Ministries of Internal Affairs of republics, territories, regions, the All-Russian Expert Criminalistic Center (ARECC) of the Ministry of Internal Affairs of Russia, expert criminalistic centers of republics, territories and regions.

When identifying a person or persons who committed a crime in the computer area, in our opinion and based on the analyzed materials of archived criminal cases, the following records from the criminalistic registration system could be used:

– persons sentenced to deprivation of liberty in Russia (surname fingerprint registration (Cartoteka IS, ADIS), surname file cabinet);

– persons sentenced to deprivation of liberty in a foreign state and extradited to Russia;

– registration of persons of operational interest to law enforcement agencies (detainees, suspected of committing crimes), including those related to computer crimes;

– persons put on local, federal or international wanted lists (AIS "FR. Opoveshenie", AIS "Crime and Search"): established persons, who committed crimes and are hiding from investigation and trial; persons, who disappeared for no apparent reason; persons, who escaped from custody, arrest or places of deprivation of liberty (including registration of especially dangerous criminals in ABD, AISS "Dosye"), evading payment of court fines for claims by organizations and enterprises, private individuals;

– persons sentenced to suspended deprivation of liberty with deferral in the sentence execution.

When analyzing criminal cases during leads presentation and verification in order to establish crimes and offenses similar in "criminal style", it is advisable, in our opinion, to use the following records in crime detection and investigation:

– records of undetected crimes and detected crimes with a characteristic method of commitment using computer systems or tools (including mobile communications);

– offenses and crimes of a certain category ("Violence": type of crime, signs of a certain crime);

– offenses and crimes committed by foreign citizens, stateless persons and Russian citizens permanently residing abroad, as well as in relation to them.

In the course of detecting and investigating crimes related to computer equipment and digital exchange of information, the following investigative actions are executed: incident site inspection, inspection of objects (including computer tools, storage media, servers, etc.) and documents; interrogation of witnesses, suspects, accused; search and seizure; investigative experiment; presentation for identification; testimony verification on site. During these actions, information about material evidence objects, traces and information obtained appears and is being checked. The most significant could be established through appropriate records of the expert criminalistic service and information centers. Thus, when identifying fingerprints, the following resources are used:

– dactyloscopy registration;

– tracking (registration) of fingerprints seized from undetected crime sites.

If an unknown person, his photo or video image appears in the case, it is recommended to use the following resources: registration for signs of appearance based on video recordings; photo library of famous criminals by type of crime; photofit file cabinets (subjective portraits, drawn and compositional portraits) of unknown criminals disappearing from the incident and undetected crime sites.

If during the course of certain investigative actions micro-objects of various nature were discovered and seized, in our opinion, the following records could be attracted: micro-objects from undetected incident sites, file cabinets and collections of the most typical

materials and substances of a certain category (varnishes, paints, paper, fabrics, fibers, soil, human biological discharge, etc.). These records exist on the basis of expert criminalistic units of the Ministry of Internal Affairs of Russia and are included in the block of reference and auxiliary records and data banks.

Consequently, during initial and subsequent investigative actions and operational search actions and with careful attention to the case and promptness in the investigation subjects work, this information array could provide significant grounds in ensuring detection and investigation of a crime related to the use of computer technologies and tools.

Relying precisely on information, including the evidence base, obtained also from the criminalistic registration system of the Ministry of Internal Affairs of Russia makes it possible to significantly increase the effectiveness of subsequent investigative actions, tracing and exposing a criminal, crime detection and case completion as a whole.

5 Conclusion

Summing the results of studying the problem on improving organization and tactics of conducting separate actions in investigating crimes in the computer information, we would propose in conclusion the following provisions significant in our opinion:

First element of the crime investigation algorithm of this type is related to importance of inspecting the incident site. This is due to the fact that the crime specific nature implies firstly obtaining sufficiently detailed information on the event, for example, through a survey (detailed explanation) of the applicant (victim, who, in turn, could be working in the network on the basis of an agreement with the provider company), clarification of the damage caused (material damage amount, method of crime, time of its commitment, possible persons involved (interested) in it and of other circumstances. Many of these issues are resolved by inspecting the incident site. Preparation for an investigative action before involving the investigative operations group includes the following actions:

− possible coordination of the incident site place and time inspection with interested persons (applicant-victim, provider representative), on the one hand, as well as with the duty service and the operations department, on the other;

− selecting and ensuring participation of specialists able to provide significant assistance during the incident site inspection;

− ensuring involvement of witnesses of the investigative action disinterested by law;

− preparation for use of video and scanning computer equipment, which would help in inspecting, recording and saving the evidence information found;

− briefing the members of the investigative operations group with distribution of their duties during inspection and outlining particulars of handling computer equipment and behavior of all those present during the inspection;

− in some cases, when inspection objects are allegedly known, conducting preliminary oral consultations with the participating specialists.

It should be noted that video and computer scanning equipment (for example, duplicators used for copying information from the computer being inspected) involved in the incident site inspection are usually on hand with appropriate specialists or with an investigator specializing in detection of this type of crimes.

The role of specialists involved in the incident site inspection including, as a rule, programmers, is currently significantly increasing. This is due to technical nature of the inspection, use of various criminalistic and computer equipment (devices) during its conduct, which assists in inspecting, fixing and saving evidence found in this case, including traces of the crime.

During the computer location inspection (the so-called workplace), the investigator should concentrate on surrounding environment, state of adjacent surfaces and location of

windows, doors, locks and premise signaling devices for finding the traditional criminalistic traces: trasological material (fingerprints, sweet and fat traces for DNA analysis), smell, tools, legs, clothes, blood, human biological secretions, etc. Moreover, particular attention should be paid to finding traces on the surface of keyboard, mouse and computer case. It is recommended to efficiently use special technical means to identify the computer personal, which include electronic cards, activator keys (access to PC) with microprocessor and memory, fingerprint identifiers (for example, Calspan), etc.

A major role being a potential source of evidence or means of evidence in crimes of this type is played by such element of the investigation algorithm as the court expertise usually assigned after the incident site inspection. Depending on the type of traces that could be left by the criminal (criminals) at the incident site involving computer equipment, its communication facilities and premises (where it is located or adjoins them), in our opinion, it is possible to include the following types of court expertise: court computer technical expertise (CCTE); court telematics expertise; court dactyloscopy and poroscopic (ejectoscopic) expertise; court trasological expertise of footprints (shoes); court trasological (mechanoscopic) expertise of hacking instruments and tools, production mechanisms of their traces; court trasological expertise of establishing previously whole in parts; court trasological expertise of locks, locking mechanisms and signaling devices; author related court expertise; linguistic court expertise of written and oral texts on any information carriers; graphic handwriting analysis court expertise; technical and criminalistic court expertise of documents and their parts; phonoscopic court expertise; expertise of objects (including micro-objects) of fibrous nature (CEMSP); court expertise of perfumes and cosmetics; court electrotechnical expertise; court medical expertise of material evidence of biological origin (blood, saliva, sweat, hair, skin); medical molecular genetic court expertise of material evidence of biological origin (human biological traces); biological court expertise of human odor traces (biological olfactory expertise).

Considering the conduct of separate investigative actions in detecting crimes in computer information technologies, it is impossible not to note such a problematic issue in the algorithm of actions based on the conduct results, including the mentioned incident site inspection, as the use of information from the criminalistic registration system of the Ministry of Internal Affairs of Russia. According to our research results, introduction of more than 15 types of records and data banks of the information system of the criminalistic registration system of the Ministry of Internal Affairs of Russia is proposed.

Thus, study on the issue of improving organization and tactics algorithm in conducting separate investigative actions during investigation of crimes in the computer information area would improve, in our opinion, and expand scientific applied capabilities of the problem under consideration.

References

1. A. Kuanysh, B. Yerlen, T. Zhazyra, European science review **1-2**, 111-112 (2015)
2. Ch. Rigano, *Using Artificial Intelligence to Address Criminal Justice Needs* (2018) https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs
3. T. Hertley, *Research and improvement of the PPSZ algorithm for SAT* (2010) DOI:10.3929/ethz-a-006206989
4. https://www/advgazeta/ru/cybercrime is becoming more and more, but its detection is decreasing

5. E. Kravets, Y. Steshenko, A. Likholetov, D. Kairgaliev, D.V. Vasiliev, Performed Using Information and Communication Technologies **466**, 585-592 (2014) 10.1007/978-3-319-11854-3_51
6. A.V. Kasatkin, *Tactics in collecting and using computer information in crime investigation: autoref. dis…. Cand. of Legal Sciences* (Moscow, 1997)
7. A.L. Osipenko, *Fight against crime in global computer networks: international experience* (Norma, Moscow, 2004)
8. N.G. Shurukhnov, *Investigation of illegitimate access to computer information. Tutorial* (University of the Ministry of Internal Affairs of Russia, Moscow, Moscow, 2004)
9. E.R. Rossinskaya, *Court expertise in civil, arbitration, administrative and criminal proceedings* (Norma, Moscow, 2005)
10. N.G. Shurunov, *Criminalistics: textbook* (MPSI, Moscow, MODEC, Voronezh, 2011)
11. M.N. Ali, Crime Detection using Digital Forensic Technology. International Journal of Computer Science and Information Security **14(10)** (2019)
12. V.B. Vekhov, S.A. Kovalev, Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia **1**, 38 – 41 (2012)
13. V.B. Vekhov, Expert-criminalist **4**, 2–4 (2013)
14. V.B. Vekhov, S.A. Kovalev, International journal of experimental education **10-2**, 185-186 (2015)
15. V.B. Vekhov, V.F. Vasyukov, Russian investigator **3**, 11 – 15 (2018)
16. V.B. Vekhov, Criminal proceedings: problems of theory and practice **3**, 5-8 (2019)