Judicial technical expertise methods for investigation of cybercrimes

V I Petrenko, A S Bereznitsky, M G Ogur, E A Nekrasova
North-Caucasus Federal University, Stavropol, Pushkin str., 1, 355017, Russia
E-mail mogur@ncfu.ru

Abstract Computer technical expertise is rather new sort of the expertise which are carried out within criminal, civil and arbitration proceedings. And though separate expertise of computer means was carried out and earlier, "computer crimes" laid the foundation for all-round development of judicial computer technical expertise as independent sort of examination. Its emergence is caused by growth of use of computer and information systems in our country in recent years.

Keywords: forensic; criminalistics; computer technical expertise; investigation of incidents.

1. Introduction
The purpose of conducting computer technical expertise (further - CTE) is protection of the rights and freedoms of citizens and the interests of the state by means of evidence-based examinations and expert researches. The special knowledge used in process carrying out CTE is knowledge in the following scientific areas: electronics, electrical equipment, information systems and processes, radio engineering and communication, computer facilities (including programming) and automation. A basis a procedural form of use of special knowledge in the field of computer technologies is judicial computer technical expertise [1-7].

2. Problem research:
Computer technical expertise as a separate sort of judicial examinations it began to be formed spontaneously in the mid-nineties, way as it usually and happens, productions of separate unique examinations. During this period the subject and problems of JCTE, its terms framework, specific division were not still formulated. There was no uniformity even in the name of examination.

One of the first publications in Russia on the matter was S.A. Katkov, I.V. Sobetsky and A.L. Fedorov's article who suggested to call this examination program and technical, however such name was too narrow and did not answer all circle of the tasks solved by this examination. There were also other names of judicial examination of this sort: information and technological examination, computer and technological examination, engineering and computer, judicial and cybernetic examination, etc. In 1996 it was offered to E.R. Rossinskaya to call this sort of judicial examinations computer technical expertise and to include it in a class of technical examinations as the computer facilities are obliged by the birth to technical sciences. In the presents time this term became standard and the discussion about the name of this sort of judicial examinations can be considered complete. Confirmation of the end of a discussion on the matter can be considered addition of "computer technical expertise" in the list of new childbirth
of the expertise which are carried out by the judicial and expert institutions (JEI) of the Ministry of Justice of the Russian Federation according to order N 237 of December 27, 2012. "About the approval of the list of childbirth (types) of the examinations which are carried out in the public judicial and expert institutions of the Ministry of Justice of the Russian Federation, and the list of expert specialties on which the right of independent production of judicial examinations in the public judicial and expert institutions of the Ministry of Justice of the Russian Federation is granted". According to this order the computer technical expertise is officially regulated for carrying out in the SEU system on the instructions of vessels, prosecutor's office, bodies of the Ministry of Internal Affairs and so forth.

Thus, judicial computer and technical examination - the independent sort of judicial examinations belonging to the class technical. JCTE is carried out for: determination of the status of an object as computer means, identification and studying its role in case in point and also gaining access to information on carriers of data with the subsequent its comprehensive investigation. A subject of scientific bases of JCTE are regularities of formation and a research of computer systems and the movement of computer information.

Patrimonial subject JCTE are the facts and circumstances established on the basis of a research of regularities of development and operation of the computer means providing realization of information processes which are recorded in materials of a criminal, civil, arbitration case and case of administrative offense.

Specific classification of JCTE is organized on the basis of providing a component of any computer means (hardware (technical), program and information support). Proceeding from it in judicial computer technical expertise are allocated [1-7]:

- Hardware and computer examination:
  
  The essence of this examination consists in carrying out a research of technical (hardware) means of a computer system. A subject of JCTE of this type are the facts and circumstances established on the basis of a research of regularities of operation of hardware of a computer system - material data carriers about the fact or an event of a criminal or civil case.

- Program and computer examination:
  
  Subject are regularities of development (creation) and application (use) of the software of the computer system presented on a research for establishment of the truth on business. The purpose of program and computer examination is studying functional purpose, characteristics and the realized requirements, an algorithm and structural features, current state of the software of a computer system presented on a research.

- Information and computer examination (data):
  
  The purpose of information and computer examination is search, detection, the analysis and assessment of the information prepared by the user or generated (created) programs for the organization of information processes in a computer system.

- Computer and network examination:
  
  Subject of computer and network examination a research of the facts and circumstances connected with use of network and telecommunication technologies.

  Such division into types of JCTE most fully covers technological features and operational properties of the objects of examination shown for a research. This classification allows already at early stages of formation of examination differentially to approach developments of methods and techniques of an expert research. At the same time such approach to JCTE can be effectively used during the assigning of complex examinations and the decision of the big list of tasks.

Practice shows that the main types of judicial computer technical expertise described above by production of the majority of expert researches are applied in a complex and, most often, consistently. Therefore, now, the patrimonial name of examination is specified in resolutions and definitions on production of judicial examination, i.e., “to appoint judicial computer technical expertise”.

It is possible to distinguish from the main objectives resolved by judicial examinations:

- Identification tasks, i.e., identification of an object for its displays.
3. The tasks solved by computer technical expertise

When determining diagnostic tasks, not only properties and a condition of an object of judicial computer technical expertise, but also the mechanism, processes and actions by results of application (use) of computer means at crime commission are investigated. And identification problems of CTE aim to establish the fact of individual and concrete identity or the general group accessory of the presented objects of examination. Let's consider tasks solvable each of the types of computer technical expertise described above.

1. Standard research problems of computer hardware objects:
   - definition of a look (type, brand), properties of the hardware and also its technical and functional characteristics;
   - determination of actual state and serviceability of the hardware, existence of physical defects;
   - determination of structure, the mechanism, a circumstance of an event due to use of hardware;
   - definition of conditions of application of hardware;
   - establishment of a causal relationship between use of concrete opportunities of hardware and results of their application;
   - definition of conditions of application of hardware, recovery of the chronological sequence of their use, scene of action and functioning.

2. Standard research problems of program objects:
   - definition of the main characteristics of the operating system, identification and research of functional properties and software configurations, time of its installation;
   - determination of actual state of a program object;
   - identification of signs of the relation ON to system or applied;
   - establishment of an initial condition of the program;
   - diagnosing of an algorithm of the software product, types of the tools used at its development and also types of the supported hardware-software platforms;
   - definition of the purposes and conditions of change of properties and a state ON.

3. Standard research problems of information objects:
   - establishment of properties and a type of the provided information in a computer system at its direct use;
   - determination of actual state of information, clarification of existence or absence of deviations in it from a standard object of JCTE;
   - establishment of an initial condition of information on the carrier of data;
   - definition of time, chronological sequence of impact on information;
   - definition of conditions of change of properties of the studied information.

4. Standard research problems of the computer network and its component:
   - determination of properties and characteristics hardware and software;
   - identification of properties and characteristics of the computer network, establishment of its architecture, configuration;
   - definition of the reasons of change of properties of the computer network;
   - the researches connected with Internet-technologies.

It should be noted that all tasks can be detailed as well for each concrete stage of an expert research. Expert problems of judicial computer technical expertise are concretized by production of each examination. They are not identical to the questions formulated in the resolution or definition.
Sometimes several questions, raised before the expert, conduct to the solution of one expert task. To the contrary, one question can require the solution of two and more independent tasks.

The essence of the judicial computer technical expertise belonging to the class of engineering technical expertise consists in studying properties and conditions of objects of examination, a research of mechanisms, processes and actions by results of use of computer means in any given crime (including computer) and also to materials of a civil dispute, administrative offense.

The objects investigated by the expert of JCTE differ not only on the natural and technical characteristics, functional purpose, but also in the status. Besides, for considerable number of objects of JCTE (the computer - the hardware block - the program - data) this situation is defined insufficiently accurately and differently in various legal acts. Any concrete object is individual and unique, it defines specifics of a certain expert research. Applicable JCTE can formulate the following definitions:

Patrimonial (specific) object of JCTE - a certain category of the objects having the general signs and relating to computer means. One of important features of an object of JCTE is its compound character.

Concrete object of JCTE - the certain computer means investigated in the course of this examination, having signs of identity and originality as defines specifics of a concrete research [8].

Now the system of objects of judicial computer technical expertise is divided according to the specific division and looks as follows:

Class of hardware objects:
- personal computers;
- peripheral devices;
- network hardware (servers, workstations, active equipment);
- the integrated systems (organizers, pagers, mobile phones);
- any components all specified a component.

Class of program objects:
- system software;
- auxiliary programs;
- development tools and debugging of programs;
- application software.

Class information objects:
- the text and graphic documents made by means of computer means;
- given in multimedia format;
- information in formats of databases and other applications.

Class objects of the computer network and its component:
Subject to application of special knowledge can be quite different
- from computers of the users connected to Internet to various resources of the supplier of network services (provider) and the information services provided to them (e-mail, service of electronic announcements, teleconferences, WWW-service and so forth)
- servers; - workstations; - active equipment.

The special interest is of conducting judicial computer technical expertise within arbitration process where CTE is shown in new contents - as normative and technical examination. However, recently, the trend of conducting similar examinations and within criminal proceedings was outlined. A subject of such examinations, in most cases, this establishment of the facts of compliance (or discrepancies) technical documentation of a system - documentation regulating its development according to state standards on information technologies. A basis of this examination is the contract signed on production or processing of a computer system or on performance of other work with transfer of its results to the customer. If the customer after acceptance of a computer system, found in it any given shortcomings and between the customer and the performer there was a dispute, then upon the demand of any of the parties JCTE can be appointed [9].

3.1. The issues resolved within judicial computer technical expertise

By production of judicial computer technical expertise, the following issues can be resolved:
The approximate questions resolved by judicial hardware and computer examination is the following: Whether the presented device belongs to hardware computer means? To what type (brand, model) does the hardware belong? What its technical characteristics and parameters? What functional purpose of the hardware? What role and functionality of this hardware in a concrete computer system? Whether this hardware belongs to the presented computer system? Whether this hardware for the solution of a specific functional objective is used? What actual state it (is serviceable/is faulty, efficient/is disabled) the presented hardware? Whether there are in it defects? Whether malfunction of this means is a consequence of violation of certain service regulations? Whether the presented hardware is the data carrier? What type (type, model, mark) of the presented data carrier? The approximate questions resolved by judicial program and computer examination is the following: What general characteristic of the presented software of what component (software) it consists? Whether traces of overcoming protection have software? What name, type, version, type of representation (obvious, hidden, remote) software? Whether this software for the solution of a certain functional task is used? What actual state of the software, its working capacity on realization of separate (concrete) functions? Whether the software has protective opportunities (program, hardware-software) from unauthorized access and copying? Judicial information and computer examination (data) is made for permission of the following questions: What properties, characteristics and parameters (volumes, dates of creation change, attributes, etc.) have data on the data carrier? What look (obvious, hidden, remote, archive) information is available on the carrier? To what type do the revealed (certain) data belong (text, graphic, the database, the spreadsheet, multimedia, etc.)? What data on the owner (user) of a computer system (including names, passwords, access rights and so forth) are available on data carriers? What initial condition of data on the carrier (in what look what contents and with what characteristics, attributes there were certain data before their removal or modification)?

3.2. **Requirements, to the questions which are taken out on permission of judicial computer technical expertise**

1. At statement of question, it is necessary to avoid slangy and semi-professional terms, they have to contain the settled conceptual framework.
2. The formulation of a question has to be accurate and unambiguous.
3. The formulation should not concern stages of carrying out a research (for example, it should not be specified that to copy the found information on a disk as it is an obligatory stage of information research).
4. Questions should not have legal character and go beyond competence of the expert.
5. Questions should not have help character.
6. Questions have to correspond to the technical base which is available in expert establishment and modern level of methodical providing.
7. Questions have to correspond to the physical evidence produced on a research.
8. Questions have to be directed to establishment of specific circumstances of the investigated event.
9. Statement of questions is allowed in that look that at their decision the costs of their decision (financial, technical, temporary and so forth) have to be minimum.
4. Perspective of investigation of information crimes

Crime in the field of computer information represents special type of crime connected with use of the automated systems, software for illegal receiving, transfer or destruction of information resource. The complexity of their investigation consists in lack of tangibility and visibility of specific responsible for crimes. Besides the staff of investigating authorities more often should face the types of crime new, not known earlier having not clear origin and possibilities of causing damage.

To define a circle of the problems connected with crimes in the sphere of computer information once their category investigates which in detail are considered in Chapter 28 of the Criminal Code of the Russian Federation. This head carries to the considered group of crimes:

- Illegal use and access to information resource;
- Development, use, distribution and introduction of virus electronic programs;
- Violations in the field of storage, transfers and processing of information flows;
- Illegal actions for the purpose of infliction of harm to a critical information system and structure of the Russian Federation.

The first category of criminal actions represents corpus delicti which is covered by Article 272 of the Criminal Code of the Russian Federation. At the same time this article defined more concrete list of the crimes connected with computer information.

In their structure, in particular, it is allocated:

- destruction of the information massif, change, blocking. The fact of recovery of data has no legal value subsequently.
- blocking of the information massif. The lawful user has no opportunity in an operating mode to carry out work.
- modification - illegal impact on parameters of information resource.
- copying - preservation and transfer of the classified information on the isolated object of storage (copying, photo fixing).

During creation of the automatic copy a system, in the absence of intention, the person is not subject to prosecution. The person who committed a crime by negligence can be brought to responsibility at commission of this group of crimes or it is deliberate.

The law enforcement official at the same time, establishes connection between deliberate act and criminal result. At its absence the sentence cannot be imposed to the person. It is worth explaining that the considered sphere is regulated also by other laws.

So since 01.01.2018 FZ-187 "About safety of critical infrastructure of the Russian Federation", also in the Criminal Code of the Russian Federation took effect, Article 274.1 of the Criminal Code of the Russian Federation which violation attracts responsibility for the guilty person was enacted. This article brought explanation that object of crime in the sphere of computer information - the public relations which provide safe functioning of electronic systems of the Russian Federation.

The guilt is expressed both by active actions of the user, and his inaction. The special subject made responsible on the qualifying sign - the lawful user allowed to an electronic system owing to official position.

The complexity in investigation of this group of crimes consists first of all in their qualification as investigating authorities have to possess special knowledge of the field of electronic technologies.

Specialists of investigating authorities besides have to have knowledge connected with the forbidden introduction in Internet network, copying, violation of ways of storage of information, breaking of systems, development, introduction of special programs.

The harmful product influences information resource of infrastructure of institutions and organizations of the Russian Federation with any form of ownership for the purpose of infliction of harm or generation of profit.

When carrying out investigative actions on this category of crimes it is necessary to consider the following nuances:

- in advance it will be prepared for withdrawal of the data carrier on which this information as it, as a rule, contains penetration traces which study will help to establish authentically a way and time
was stored, and also the place from which penetration is made is possible.

- to arrive to the place as soon as possible to limit access for all persons to this device. It is connected with the fact that, as a rule, the staff of the company is either criminals, or accomplices of crime, and can try to hide traces of crime.
- to disconnect the device from network to protect it from repeated intervention through remote connection.
- to try not to conduct independently before withdrawal any manipulations with the equipment if it is impossible to be sure of result of any given action. Withdrawal of the carrier has to be made according to requirements of the Criminal Procedure Code of the Russian Federation. After the equipment which underwent unauthorized access was seized it is necessary to pay attention to personnel of the company, especially to persons who are engaged in service of the COMPUTER, maintenance of network and information security.

As the main suspects at the first stages of preliminary investigation those employees who meet the following criteria act:

- knew or could know that on this device information which is of a certain value is stored;
- have the high skill and special knowledge which are allowing or presumably giving the chance of commission of this crime.

Special attention experts who are engaged in information security from unauthorized access as they, as a rule, independently "write" the programs directed to information security deserve and know everything their weak and strengths. Besides the employees working in the company, it is necessary to pay also attention to those who worked in it earlier and presumably corresponded to those criteria which were listed above, both under the employment contract, and on civil. As a rule, there will be enough these measures to solve this crime. Nevertheless, cases when the criminal has extensive experience and the latest technologies sometimes meet, never worked in this company, and worked, for example, by the order or aiming. Such hackers in Russia of unit, but, nevertheless, they are.

For disclosure of the crimes committed by them hardly law enforcement agencies will have enough experience and opportunities. The consequences of violation of the rules of storage, use, information transfer similar to the previous articles - harm to the victim in the form of loss of information, violation of privacy of data, blocking and change of volume.

By the first part of Article 274 of the Criminal Code of the Russian Federation the punishment term up to 2 years, on condition of causing large damage is provided. At qualification of act the investigating authorities define what norms of criminal law on information security were violated by the guilty person and what consequences his actions entailed, establish a fault form.

Errors of the investigation and court at prosecution and qualification of actions lead to the termination of criminal cases and release from responsibility of guilty persons.

So, for example, the guilty convict according to Article 272 of the Criminal Code of the Russian Federation was exempted for access to official information and causing damage of the organization from liability by superior court, having specified that the special subject - the person who has lawful access to the COMPUTER and an information system is brought to responsibility. Negative consequences were caused by failure to follow security guidelines and neglect of the duties. Actions need to be qualified according to Article 274 of the Criminal Code of the Russian Federation.

In this situation the system administrator of establishment during the work did not use a security system. Copying of information with personal data of employees and personal contacts of commercial partners was as a result carried out. Criminal case was mistakenly brought according to Article 272 of the Criminal Code of the Russian Federation and brought to trial. The decided adjudication was repealed by supervising instance, criminal case is dismissed, on circumstances of the expiration of terms of criminal prosecution. Investigating and judicial authorities did not consider that a crime was committed by a special subject - the lawful user. Actions needed to be qualified according to Article 274 of the Criminal Code of the Russian Federation.

The given examples prove complexity of disclosure of computer crimes for law-enforcement bodies. There is a need of production of information and technological examinations.
In expert way also existence of corpus delicti in actions of persons as neither the court, nor for participants of process often has special knowledge of the field of modern electronic technologies is possible to establish the legal facts.

It is obvious that the edition of special instructions which will allow to understand effectively features of this type of crime is necessary and will give the criminalistic analysis of these acts as it was made at the time for other types of crime.

For today such crimes are rather a nonsense, than routine work of law enforcement agencies. Nevertheless, in criminalistic science exist already today, though very poor, based on experience of the advanced countries data allowing to sketch a technique of investigation of these crimes. On the basis of knowledge gained during clarification of the above-mentioned questions the investigator has to have a clear picture of crime.

The circle of subjects which are capable to get unauthorized access to the closed servers or networks of the company is extremely limited because the criminal in this case has to have huge knowledge base in the field of computer science and information security [8-10].

5. Conclusion
Investigative practice shows that the more difficult technically the way of penetration into a computer system or network, is easier to allocate those the suspect as the circle of the experts having the corresponding abilities is usually limited even more. Solvability of computer crimes in the Russian Federation now quite low. It is connected with the fact that law enforcement agencies meet this type of crime extremely seldom and therefore real practical experience and a technique of investigation of these types of crime by them it is not developed yet.

At the same time, in most the companies there are no expensive modern programs and other means of information protection that does them vulnerable for the attacks of hackers. Most likely, the situation with these crimes will shortly change.

At the present stage in Russia everywhere electronic document flow, the electronic auction, online of the request for rendering services actively takes root. All this is attracted, on the one hand, by acceleration of processes of filing of applications, and with another - transfers them to less protected reality - virtual that enhances risks of information leakage from the computer in bases of malefactors.

References
[1] Constitution of the Russian Federation (of 12.12.1993).
[2] Federal law of the Russian Federation "About Information, Information Technologies and on Information Security" (No. 149-F3 of 27.07.2006).
[3] Doctrine of information security of the Russian Federation (No. Pr-1895 of 06.09.2000).
[4] Federal law of the Russian Federation "About the State Secret" (No. 5485-1 of 06.10.1997).
[5] Decree of the Russian President "List of Data of Confidential Character” (No. 188 06.03.1997).
[6] Federal law of the Russian Federation "About Personal Data” (No. 152 of 27.07.2006).
[7] Federal law of the Russian Federation "About the Digital Signature" (No. 1-FZ of 26.12.2001).
[8] Carrier, B. 2019 Open Source Digital Forensics Tools
[9] Olajide F, Savage N, Ndzi D, Al-Sinani H 2019 Forensic Live Response and Event Reconstruction Methods in Linux Systems
[10] Thomas, D.S.; Forcht, K.A. 2004 Legal methods of using computer forensics techniques for computer crime analysis and investigation (Issues Inf. Syst) pp 692-698.
[11] Lillis, D.; Becker, B.A.; Scanlon, M. 2016 Current Challenges and Future Research Areas for Digital Forensic Investigation (Proceedings of the 11th ADFSL Conference on Digital Forensics, Security and Law, Daytona Beach, FL, USA, 13 April 2016) pp. 9-20.
[12] Prasad, M.A.R.; Satish, Y.N. 2013 Reconstruction of Events in Digital Forensics (Int. J. Eng. Trends Technol. 2013, 4) pp 3460-3467. [CrossRef]
[13] Carvey, H. 2009 Windows Forensic Analysis DVD Toolkit 2E (Syngress: Burlington, MA, USA)
[14] Harrell, C. 2011 What’s a Timeline. Available online:
http://journeyintoir.blogspot.com/2011/09/whats-timeline.html (accessed on 28 May 2019).

[15] Esposito, S.; Peterso, G. 2013 *Creating Super Timelines in Windows Investigations* (Proceedings of the 9th International Conference on Digital Forensics, Orlando, FL, USA, 28-30 January 2013) pp 135-144.