UDC 621.3

O.V. Ribalsky,

Doctor of technical sciences, professor,

L.M. Timoshenko,

A.Y. Mushchak

COMPUTER AND TECHNICAL EXAMINATION AND INFORMATIONAL SECURITY

An interaction between judicial examination of computer systems and telecommunication networks with planning, creation and researches of the complex system of information security in such systems and networks is considered. Mutual use of theoretical and practical investigations, realized in both sciences, is offered.

Keywords*: information security, criminalistics, judicial examination, computer systems, telecommunication networks.*

Quite often many types of forensic examinations related to information processes, tightly intersect with issues of information security and in fact there are sometimes surprising aspects. In such examinations may include, for example, monoscopically expertise, where forensic questions of authenticity of the records is also the aspect of protection of the state bodies and the public from misinformation [1].

Careful forensic examination of the issues of computer-technical expertise (regarding subsection), and allows it to be attributed to the same kind of expertise. In a separate genus examinations it was highlighted recently when the need for forensic investigations of computer equipment and process there have necessitated the involvement of qualified professionals, conducting the necessary theoretical groundwork and create special methods and tools for its implementation. It should be noted that both the theory and development of methods and tools for such assessments are currently in the early stages of its development, because the question of its separate type of examination is started up only in the 90-s of XX century [2–4]. Objects such expertise are computer-based tools: hardware; software objects and information objects (data)" [3, 4]. In [3, 4] provides a

definition of the subject of such examination, that “there are facts and circumstances, determined on the basis of the analysis of the regularities in the development and operation of computer means of ensuring the implementation of information processes, which are recorded in criminal, civil cases, cases on administrative offences”. In [5], according to their objectives and specifics of the study identified the following types of examinations: – hardware-computer expertise, the subject of which is the actual data set in the study of technical (hardware) computer system; – software and computer expertise, the subject of which are the laws of creation and use of software systems, presented at the research; – information and computer expertise, as the main type regarding subsection, the subject of which is the establishment of the actual data in the course of the search, detection, analysis and evaluation of information prepared by the user or generated by the software for the organization of information processes in a computer system”; – computing and networking expertise, the subject of which includes the study of the facts and circumstances associated with the use of network and telecommunication technologies, the task of the investigator (the court) to establish the truth; – telecomunication examination, “the subject of which is the actual data, are set on the basis of special knowledge in the study of telecommunication and communication facilities as material carriers of information about a fact or event of any criminal or civil case”. We believe that species such as computer and network expertise (CME) and telecommuncation examination (CED) directly related to information security as a separate entity or object, and the state as a whole. Note that until the General objectives of information security is to protect information against threats of any action for violation of its integrity, destruction, modification, or theft (as well as the creation and spread of misinformation). These tasks are set as in the development of technical specifications for the design, and the design of complex information security systems in computer systems and telecommunication networks. It is necessary to provide the total number of ways of protection. To them in the first place, should include protection against unauthorized access, virus protection,

protection against information leakage through technical channels, and others. Of course, for each individual object protection will apply a specific security profile, which involves individual detail of these areas, taking into account characteristics of the object of protection and information, which is processed in the system. Studies provide a given level of security of information in the system, carried out on special techniques, which aim at determining compliance with the specified profile and level of protection. Now consider the list of questions [6], which, as a rule, are the experts when conducting CME, TCA. Hosted access to telecommunication systems, and how? Resources and information in a telecommunication system, and how? Was the transmission (reception) of information in a telecommunication system, and how? Are there any signs of interference in the operation of telecommunication systems? Could the hardware be combined in a telecommunication network, and on what grounds? To establish the routing path of data in a telecommunications system. Whether used in programs passwords and dentify-CIN codes that were entered by the user. What software is used for the operation of a computer network? Is it licensed? How is the connection of the computers on the network? Is there a solution to the global computer network? What computers are servers (mainframe computers) network? How is the transmission of information on this enterprise, institution, organization, firm or company on nodes of a computer network? Used to restrict access to information computer network passwords, identification codes? How are they used? Are there any faults in the individual programs, individual computers when they are functioning as part of the network? What are the reasons for these failures? What information is transmitted, processed, and manipulated using a computer network? Perhaps the use of telecommunication tools (equipment) for these purposes? What is the purpose of software products? To solve some applied problems they are intended? What methods of input and output information used? Whether the results of running the programs necessary actions? What software information protection methods are used (passwords, identification codes, programs, protection, and so on)? No attempt is made password mining or other

attempts of unauthorized access to computer information? What information is contained in hidden files? What technical devices are used to protect computer information? What are their specifications? Available technical documentation for these products? Answer options devices to those described in the documentation? Did any protection software modifications or physical pressure. Used or no artificial means of information protection? Are there presents on magnetic media erased (deleted) files? Yes, what are their names, sizes and dates of creation, the duration of removal? You can restore previously deleted files and their contents? Changed the contents of the files (indicate which)if Yes, what was the outcome? In what form is the information about the results of anti-virus programs, programs to verify file checksums? What is the meaning of this information? Whether the presence of failures of individual programs? What are the reasons for these failures? In what condition are the files contained on magnetic media? When I made the last adjustments to these files? In what files a program referred (indicate which) presented on native media, and what information files it created? Does the media information (specify what information is interested in)? Yes, what is it? Contains media studied computer information about specific (specify which) user actions? Attempts were carried out the destruction of this information? Did the investigated drive specific procedures for destruction of information? Created the information on the computer or transferred from one medium to another? How information (specify what kind) are transferred to the investigated computer (media)? What technology and the chronology of the electronic document (specify electronic document)? Date and time of creation (printing, deleting, adding, etc) files to specify the content)? Whether it contains drive information of the investigated computer specific (specify what) software? How and when this software is installed? In the analysis of these issues becomes apparent their intersection with the goals and objectives arising from the design, development and research of isip. And in cases of threats of information leakage and identify any weaknesses in the protection of these issues in a very direct way. Thus, there is the so-called scientific “joint” between the solution of the problems of information

security of computer systems and telecommunications networks and forensics, conducting CME, TCA. From the history of science somebody knows that the most productive scientific and technical solutions always occurre and implement on these “joints”. Therefore, we believe that there is a direct sense in the mutual use of the best practices of each of these sciences. It should be noted that, despite the relative “youth” of such examination, it gained quite a serious software tools for practical research and measurement, as it can be seen from the above list of issues, which are solved such expertise. We believe that much of this toolkit can be used to research the real level of protection of computer systems and telecommunication networks. Moreover, we note that the main theoretical basis of criminalistics, which includes expertise, have long been developed and repeatedly proven theory of forensic identification, it is possible to accurately determine the requirements for the identification features and the validity of their use in the studies used in each specific expert technique. We believe that its application in a number of problems are to be solved when creating the isip computer systems and telecommunications networks, it would be very useful. We also believe that some of the techniques, methods and tools used in the creation of isip computer systems and telecommunication networks (e.g., methods of profiling, methods of risk assessment and the like),

From all the above mentioned it is possible to make following conclusions:

1. Expert tasks when conducting certain types of computer-technical expertise, close to the problems that are solved in the design, creation and research of complex systems of information protection in computer systems and telecommunication networks.
2. Techniques, methods and tools used in forensics and information security, could complement each other.
3. The application of theoretical and practical bases of both sciences have contributed to their mutual enrichment and development.

LIST OF USED SOURCES

1. *Рыбальский О.В.* Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе / О.В. Рыбальский, Ю.Ф. Жариков. – К.: НАВСУ, 2003. – 300 с.

2. Криминалистика : Учебник для ВУЗов / под ред. Р.С. Белкина. – М., 1999.

3. *Россинская Е.Р.* Судебная экспертиза в уголовном, гражданском и арбитражном процессе / Е.Р. Россинская. – М.,1996. – 459 с.

4. *Россинская Е.Р.* Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. – М., 2001. – 306 с.

5. *Зинин А.М.* Судебная експертиза : Учебник / А.М. Зинин, Н.П. Майлис. – М., 2002. – с. 50.

6. *Меликов А.С.* Основания назначения судебной компьютерно-технической экспертизы (компьютерной экспертизы) / А.С. Меликов [Электронный ресурс]. – Режим доступа : http://juranalytic.ru/2012/05/20/rassledovanie-kompyuternyx-i-drugix-prestuplenij/osnovaniya-naznacheniya-sudebnoj-kompyuterno-texnicheskoj-ekspertizy-kompyuternoj-ekspertizy/