Computer-technical expertise as evidence in cases of violations of bank (currency) laws

Yamnenko Tatyana

Doctor of Law,
Professor of the Department
of Civil Law and Process Educational-Scientific
Law Institute of the National Aviation University

Zhmur Nataliya

Candidate of legal sciences, Associate professor of
the Department of Commercial, Air and Space law
Educational-Scientific Law Institute of the
National Aviation University

Abstract. *This paper deals with the problems of expertise. In the article expedience of setting of different types of computer-technical examination is examined at proving of bank (currency) offences. Proposed changes to the Regulations on the appointment and conduct forensic examinations and expert research.*

Key words: *proof, banking and currency laws, computer equipment, expertise, control.*

Problem statement

With rapid development of computer technologies, virtually all operational work papers have transformed into electronic form; however, despite of all advantages of technical innovations, the computer equipment remains vulnerable to failures, and therefore, there is a threat of data loss or damage. The loss of information kept at electronic media, specifically, impossibility to provide it to inspectors during audit activities may serve the basis for holding such financial institution accountable.

The degree of scientific development of the problem. The general issues of the expertise have become the subject matter of the studies carried by such scientists as: V. I. Honcharenko, B. M. Isakovych, H. M. Nadhornyi, L. M. Romanenko, M. Ia. Sehai. The computer forensics, as a research trend, has been specifically elaborated by O. Rosinska. However, the legal basis for enshrining the computer forensics subtypes at the sectoral legislative level have not been considered yet.

The objective of the article. The purpose of the article is to establish appropriateness to assign a computer forensics, in particular, its specific varieties, in the process of proving activity in the cases on infringement of banking (currency) legislation.

Statement of basic materials. Having into account the difficulties that arise in the process of proving the facts of infringements of banking (currency) legislation, a necessary step shall be made towards extension of the forensic subtypes to be possibly assigned in

administrative cases, and making respective amendments to sectoral legislation governing the forensics activities.

At the start of the 90-ties there emerged, kept actively developed, the network of commercial banks of Ukraine. Commercial banks are the institutions carrying out its activities under the license obtained from the National Bank, at the expense of various sources, based on their established loan policy, at their risk, for the purpose to gain maximum profit from their activity [1, p. 66]. Commercial banks provide under the loan contractual conditions, cash management, and other banking service for legal entities and physical persons.

Nowadays, one cannot help imagining the world without information technologies. Killer innovations of the progress in science and technology have embraced all spheres of human activity which enabled people to simplify their work when solving certain tasks and performing specific types of work, with baking activity being among them [2, p. 46]. The opening of the computerization epoch of the banking activity stems from the 60-ties, when, on the West, there emerged the first automated system of accounting of the transactions with clients' accounts and payments on cheque. The 70-ties were marked with a certain advance in the field of automation of baking activity. This technology was widely spread not only in the account-related transactions but also in the work with clients.

Automation of banking activity was predetermined by the necessity:

– to improve service for clients, to provide them a wide range of banking services, and to attract new clients;

– to reduce operational costs of a bank and to accelerate performance of banking transactions;

– to improve management of a bank and increase its competitiveness;

– to expand a bank and to enlarge the segment of a banking market [3, p. 5].

Analyzing the state of things at the of commercial banks level, it should be noted that the extent of implementation of the latest information technologies in commercial banks of Ukraine is very diverse. This is connected with an accelerated development of the number of financial institutions and diverse level of their financial capacities in terms of implementation of computer technologies [3, p. 7]. Yet, with increased scope of banking services, the number of their branches, clients, and relations, banks have no other alternative rather having powerful computers. Computerization of banking and currency transactions has significantly facilitated the bank-and-client relations, nonetheless, such simplification has a great disadvantage as well. Even the latest computer equipment may undergo failure, out of voltage drop, if a bank does not ensure to put a high quality uninterrupted power supply in place, or due to willful (careless) interference with computer operation (for instance, interference with devices and units directly connected with its operation, and the tools of input of information by means of its displaying or transferring on a printer, etc.). Having regard to that virtually all operational work papers are kept in electronic format, there emerges a threat of its being lost or damaged, possibly leading thereby both to the infringement of banking legislation and to the impossibility for the inspecting bodies representatives to detect an offence committed or collect the facts about already detected unlawful action. This, for instance, refers to the offences directly relating to computer equipment operation (banking and currency transactions, failure to submit reports to NBU, etc.).

It should be made allowance for that it is impossible, with the unaided eye, to visually detect the fact of interference with the hardware operation as it does not leave a visible mark. Yet, there are special types of forensics designed to detect the interferences alike. In truth, such types of forensics have not been widely spread yet in the proceedings in the cases on administrative breaches. L.M. Romanenko considers that the forensics in administrative process now in Ukraine is being at the new stage of its development, as rapid development of science and technology, and the interests of case law require that the experts in legal expertise responded quickly to emerging new scientific, technical resources and special knowledge and usage thereof in the process of proving. The given type of studies extends the proving capacities of individuals and enables them to use unlimited opportunities of the latest science in the process of pre-trial consideration of cases [4, p. 13]. The basis procedural form of application

of special knowledge is a legal expertise and its types. As V.I. Honcharenko fairly notes, the delineation of the boundaries of the competences of each type of court forensics shall be in principle determined by the disciplinary classifications of sciences, as an accurately substantiated classification of court forensics, being flawless, gives rise to useful practice and contributes to objective development development of each type of forensics based on fundamental science [5, p. 246].

One of the types of forensics designed to study the issue of the computer equipment (their technical operation and informational component) is computer forensics. The Decree of the Ministry of Justice of Ukraine dated 08.10.1998 No 53/5 "On Approval of Assignment and Conducting Court Forensics and Expert Examinations and Scientific and Methodological Recommendations on Preparation and Assignment of Court Forensics and Expert Examinations" (hereinafter – Instruction) classifies it as a part of forensic engineering. Yet, the stated expertise has not come into common use as compared to other types of forensics. We think this is because the Instruction does not provide for the detailed specification of peculiarities of each of the subtypes of forensic engineering. This gap leads to that the subjects of administrative process, due to not realizing the possibilities of its being assigned, either fail to use this means of obtaining evidential information or makes an expert tasked with a study of only one of the components of computer equipment disregarding the comprehensive examination thereof.

Analyzing the foreign experience of the condition of the regulatory provision for carrying out computer forensics, there was studied the List of generic (types) of court expertise conducted in the federal budget forensic institutions of the Ministry of Justice of the RF in 2012; however, it does not foresee the detailed subdivision into subtypes either. What made the scientist O.R. Rosinska [6] to propose the additional subtypes of computer forensics in her study, the detailed description thereof and the questions the experts should be tasked with? The underlying concept of her division is a type of a component (a part of the computer equipment) subject to examination (hardware, technical, software, and dataware).

The computer forensics is used in order to obtain access to the information available at data media by carrying out a comprehensive study thereof. An impetus for assignment to carry out the expertise may be given by the inspectors' own considerations as to the situation with a functioning computer or the computer, which abruptly became faulty on the day before a scheduled/unscheduled inspection, or, even, during its being carried out. Under such circumstances, the inspectors may assign the above stated expertise. In the event if a bank representative insists on occasional nature of the failure of the bank's computer equipment, the initiative to carry out such expertise may come from such representative. The inspection may be carried out on the site where the computer equipment is located (but it should be taken into account that this will require respective software and special technical means, and certain time to carry out it) and in the premises of an expert institution. In the event of necessity to carry out the expertise on the site, the person who has initiated it is obliged to provide for an expert an access to the premises where the object of expert examination is located and to ensure proper conditions for his or her work.

And, although the computer forensics is assigned predominantly in criminal cases, we consider it to be actively used in administrative proceedings as well, as the court expertise is aimed directly at enforcement of obtaining the results of the highest evidentiary significance during examination of the hardware, software, and computer data, which speaks for its the universal nature for various branches of procedural law.

The subtypes of computer forensics, following the opinion of O.R. Rosinska, are: hardware forensics; software forensics; dataware forensics (expertise of data); and network computing system forensics [6].

The hardware forensics implies carrying out examination of technical (hardware) means of computer system. The subject matter of this type of computer forensics are the facts and circumstances established on the basis of the study of regularities of operation of the hardware appliances of computer system – the physical media of the information about a fact or event of a certain business. The example of the hardware forensics is the study of possible applications of atypical and external (for instance in the event of collision or hardover)

ways of the examination of data media (most often hard drive) in order to obtain the valuable information kept thereon [6, p. 199].

The computer forensics is assigned in order to carry out the expertise of software. Its subject matter lies in the study of regularities of development (creation) and application (usage) of the software of computer system made available for examination in order to establish the truth in a case. The software forensics aims at the studying of the functional designation, characteristics, and the requirements complied with, algorithms and structural peculiarities, current state of the software of a computer system made available for the examination [6, p. 200].

The dataware forensics (the expertise of data) is a key type of computer forensics, as it allows for making the holistic construction of the evidentiary foundation complete by means of the final solution of the majority of questions related to computer data. This type of the expertise aims at search, detection, analysis, and assessment of the information prepared by a user or created by the applications for the purpose of organization of informational processes within a computer system [6, p.201].

The network computing system forensics, unlike the above mentioned ones, is based, first of all, on the functional purpose of computer ware implementing any network technology. It stands out as a separate type because only the use of special knowledge in the field of network technologies allows for synthesizing the objects received, the data about them, and for efficient solving the expert tasks set. The expert knowledge related to the Internet-technologies are in class of their own with the system of network computing forensics [6, p. 202].

By means of carrying out a comprehensive analysis, an expert can establish the circumstances, under which the failure has taken place, and withdraw and analyze the information obtained. In view of this, we offer to actively use computer forensics in the proving process in the cases on infringement of financial legislation. However, “inclusion and application of respective methods, form, and recourses of cognition in the process of proving implies legal enshrinement thereof and recognition of such phenomena” [7, c. 77]; therefore, it would be appropriate to include the foregoing subtypes to Instruction № 53/5 and supplement paragraph 12 “Expertise of the hardware and software products” with new paragraph 12.1.1 having the text as follows:

“12.1.1. There shall be distinguished the following subtypes of computer forensics: hardware forensics; software forensics; dataware forensics (expertise of data); and network computing system forensics”.

When drafting up the list of the questions to be solved with the help of various subtypes of computer forensics applied, a national legislator shall adopt the list proposed by O.R. Rosinska as a basis.

In order to provide an example of the necessity of application of computer forensics, let us illustrate the administrative case No0417/2-a-43/2011 dated 19 January 2011, of OJSC “ACCENT-BANK” vs the National Bank of Ukraine. The plaintiff considered the Ruling of the National Bank of Ukraine No12-139/2-6 dated 19.10.2010 unlawful as, as a result of making copies because of malfunction, there were printed the documents containing no displayed data required for establishment of identity of legal entities of residents. Taking into account the scope of the document on 26 pages, it was inappropriate to check the document. The error was detected while the inspection group was working. The employee responsible for financial monitoring of OJSC “ACCENT-BANK” proposed the inspecting working group of the National Bank of Ukraine to make them personally sure in availability of these requisites in the original copy of the document kept in electronic format, which was dismissed. The court did not take into account the statements of the plaintiff and her representative about technical failure at the moment of printing of the document, as such statement had not been confirmed during the court hearing. Either, there was not proved the action of non-interference with “the electronic original of the document”, namely, its being not edited after the fact of infringement had been established.

In our opinion, if the bank representatives had initiated the computer forensics to be carried out in advance, they would have avoided being imposed a fine following the results of the inspection.

Conclusion

Thus, it may be concluded that the computer equipment is vulnerable to malfunctions leading to the loss or damage of data, which may become a reason for holding an entity accountable, and therefore, there arises the necessity to provide banks with additional resources to confirm their being not guilty. For this reason, it is proposed to actively use computer forensics in administrative process; whereas, the legal basis for its being assigned requires respective amendments to be made to operative legislation.

References:

1. Vdovenko L. O. Rol` komercijnyh bankiv v rozvytku ekonomiky Ukrayiny / L. O. Vdovenko // Zbirnyk naukovyx pracz Tavrijs`kogo derzhavnogo agrotexnologichnogo universytetu (ekonomichni nauky). – 2013. – # 1(3). – S. 65-70.
2. Ostrovs`ka N. S. Osnovni aspekty informacijno-texnichnoyi bezpeky komercijnyx bankiv Ukrayiny ta jix vplyv na spromozhnist vykonuvaty nymy svoyu misiyu / N. S. Ostrovs`ka, I. M. Yakub'yak // Finansovo-kredytna diyal`nist`: problemy teoriyi ta praktyky. – 2009. – # 1 (6). – S. 46-52.
3. Yer`omina N. V. Bankivski informacijni sy`stemy : navch. posibnyk. / N. V. Yer`omina. – K. : KNEU, 2000. – 220 s.
4. Romanenko L. M. Ekspertyza v administratyvnomu procesi : avtoref. dys. … kand. yuryd. nauk : specz. 12.00.07 «administratyvne pravo i proces; finansove pravo; informacijne pravo» / Lyudmyla Mykolayivna Romanenko // Irpin`, 2013. – 20 s.
5. Goncharenko V. Y. Klassyfykacyya nauk i sudebnaya ekspertyza / V. Y. Goncharenko, A. A. Stepanova // «Rol i znachenie deyatel`nosti professora R. S. Belkyna v stanovlenii i razvityii sovremennoj krimynalistiki» : mater. mezhdunar. nauch. konf. (k 80-letiyu so dnya rozhdeniya R. S. Belkina). – M. : Akad. upr. MVD Rossii, 2002. – S. 246-250.
6. Rossinskaya E. R. Sudebnaya ekspertiza v grazhdanskom, arbitrazhnom, administrativnom i ugolovnom processe / E. R. Rossinskaya. – M. : Norma, 2006. – 256 s.
7. Shtyx O. V. Analiz znachennya dokazuvannya v spravax pro administratyvne pravoporushennya / O. V. Shtyx // Yurydychna nauka i praktyka. – 2011. – # 2. – S. 73-79.