ISSN 1392–6195 (print)
ISSN 2029–2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2010, 1(119), p. 317–329

APPLICATION OF IT EXAMINATION IN INVESTIGATION OF CRIMES ON SAFETY OF ELECTRONIC DATA AND INFORMATION SYSTEMS

Lina Novikoviene

Mykolas Romeris University, Faculty of Law,
Department of Business Law
Ateities 20, LT-08303 Vilnius, Lithuania
Phone (+370 5) 2714 525
E-mail linan@mruni.eu

Egle Bileviciute

Mykolas Romeris University, Faculty of Law,
Department of Administrative Law and Procedure
Ateities 20, LT-08303 Vilnius, Lithuania
Phone (+370 5) 2714 545
E-mail eglek@mruni.eu

Received 3 February, 2010; accepted 20 March, 2010

Abstract. *As an EU state, Lithuania has become an active member of the eEurope 2005 initiative, implementing the goals set forth in the strategic plan for the development of information society in Lithuania. Information technologies introduced into various areas of life open up new, more convenient opportunities to receive services and information. The modernization of state management becomes an integral factor for ensuring continuous social development.*

The objective of this paper is to study practical aspects of the application of specialized knowledge in the investigation of crimes on electronic data and information systems security and to offer some recommendations for the investigation and prevention of such crimes. This article is the first of a two part study. In the next article, the authors intend to present aspects

of prevention in crimes against electronic data and information systems security.

The authors used statistical data, results of a survey of experts—investigators of crimes on electronic data and information system security, experts of information technology (IT) forensics.

***Keywords**: forensic examination of information technologies, application of specialized knowledge in the investigation of crimes against electronic data and information systems security, crime prevention, information security.*

Introduction

In 2004, Lithuania became a fully-fledged member of the European Union and entered a new stage in state development. The Government of the Republic of Lithuania adopted the National Action Programme of the Lisbon Strategy,[1] oriented towards economic growth and employment with emphasis on the development of knowledge society and innovations. Lithuania became an active participant of the eEurope 2005 initiative,[2] by implementing the objectives, tasks and targets outlined in the Strategic Plan for Information Society Development in Lithuania.[3] As information technologies are introduced into different areas of life, they open up new, more convenient opportunities to access different services and obtain information. The modernization of state governance is becoming a key factor for ensuring continuous social development.

The development of information society and information technologies does not result in positive consequences only. Individuals with criminal inclinations also find a niche. As C. Förster indicates, information technology is commonplace in modern society. Therefore, criminal investigators often initiate forensic IT examinations to decode, evaluate, and properly prepare digital evidence for a criminal procedure. This is mostly seen in the energy, financial and insurance sectors.[4] Crimes on information technology—*crimes on electronic data and information systems security*—were criminalized in Lithuania in 2000, after adopting the new Criminal Code (CC).[5] On 24 January 2004, amendments were made and two new articles were added to this Chapter, namely Art. 198(1) 'Illegal access to a computer or a computer network' and Art. 198(2) 'Illegal possession of hardware, software, passwords, log-in codes or other data, intended for the committing of crime'.[6] In June 2007, a package of amendments to Chapter XXX of the

1 Decision of Government of Republic of Lithuania of 2002 06 20, No. 670. *Official Gazette.* 2005, No. 78-2823.

2 Kažemikaitienė, E.; Bilevičienė, T. Problems of involvement of disabled persons in e. government. *Technological & Economic Development of Economy.* 2008, 14(2): 185.

3 Decision of Government of Republic of Lithuania of 2001 08 10, No 984. *Official Gazette.* 2001, No. 71-2534.

4 Förster, Ch. Der polizeiliche Sachverständige IT-Forensik. [Police IT examination-Forensic]. *Kriminalistik.* 2007, 61: 621.

5 The Criminal Code of the Republic of Lithuania. *Official Gazette* 2000, No. 74–2262, with further amendments and supplements.

6 Law on changes and supplements of 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 articles and 198(1)

CC was adopted, whereby the Chapter was renamed into 'Crimes on Electronic Data and Information Systems Security' and the shortcomings of existing laws were corrected.[7] However, criminal acts which are currently qualified under the Art. 196-198$^{(2)}$ of the CC had also been committed in Lithuania prior to the enactment of this law. These acts are rather specific due to their latency, the inherent character of these crimes, the personal qualities of the perpetrators, and the rapid development of information technologies.

Crimes on electronic data and information systems security result in dire social and economic consequences. It is, therefore, necessary to constantly improve the theoretical-methodological base of IT crime investigation, the practical investigation skills and the criminal prevention measures against these criminal acts.

The purpose of this study is to offer some suggestions for the improvement of criminal investigations and prevention measures in the area of information systems security in Lithuania. These recommendations are based on the analysis of the possibilities for the application of specialized knowledge in the criminal forensic examination of information technologies, following the example of investigation of crimes on electronic data and information systems security, and information about the development trends in the application of specialized knowledge in criminal investigations. The subject of research is quite broad. Therefore, this article presents the first part of the results of the authors' research. Ideas on the prevention of digital crimes will be presented in next article.

The objectives of this study are as follows:

1) to analyse the practice of criminal forensic examination of information technologies and to reveal their potential and the level of application in Lithuania;

2) to identify problems in the practice of criminal forensic examination of information technologies and to propose solutions to these problems;

3) to review prospects for preventive measures by experts (specialists) carrying out investigations of information technologies and ways of implementing them.

1. Criminal Forensic Examination of Information Technologies: the Problem of Definition

Compared to other criminal acts stipulated in the CC, statistical indicators for crimes on electronic data and information systems security[8] are not very high due to their latency. For instance, in January–November 2009, there were 56 criminal acts registered pertaining to electronic data and information systems security; among those, 7 acts according to Art. 196 of the CC 'Illegal tampering with electronic data', 1 act according

and 198$^{(2)}$ articles of The Criminal Code of the Republic of Lithuania. *Official Gazette.* 2004, No. 25-760.

7 Law on changes and supplements of 7, 38, 47, 63, 66, 70, 75, 82, 93, 129, 166, 167, 172, 178, 180, 181, 182, 183, 184, 185, 189, 194, 196, 197, 198, 198$^{(1)}$, 198$^{(2)}$, 199, 202, 213, 214, 215, 225, 227, 228, 231, 233, 235, 252, 256, 257, 262, 284, 285, 312 articles and titles of XXVI, XXX chapters, supplement by 256$^{(1)}$, 257$^{(1)}$ articles of The Criminal Code of the Republic of Lithuania. *Official Gazette.* 2007, No. 81-3309.

8 Department of Informatics and Connections of Home Office of Republic of Lithuania. Data concerning criminal actions, committed during January–November 2009 [interactive]. [accessed 03-02-2010]. <http://www.vrm.lt/fileadmin/Image_Archive/IRD/Statistika/html_file.phtml?metai=2009&menuo=11&ff=1G&fnr=7>.

to Art. 197 of the CC 'Illegal tampering with an information system', 31 criminal acts according to Art. 198 of the CC 'Illegal interception and use of electronic data', 11 acts according to Art. 198(1) 'Illegal access to an information system', and 6 criminal acts according to Art. 198(2) 'Illegal possession of hardware, software, passwords, log-in codes or other data'. It can be seen from this information that the majority of crimes on electronic data and information systems security are crimes stipulated in Art. 198 of the CC. The number of these crimes has demonstrated the fastest growth in 2009 (based on statistics of 2007–2009). Moreover, there was an overall growth in crimes on electronic data and information systems security.[9]

Along with the recent criminalization of these acts emerged a new area in examination and forensics—criminal forensic examination of information technologies. This field receives a number of different names in scientific literature. In the opinion of E. Rossinskaya,[10] examinations dealing with computer hardware and its components should be called computer-technical examinations, which are further subdivided into two large sub-types: technical examination of computers and their components and examination of software. Supporting E. Rossinskaja's opinion, V. Kazantsev[11] suggests supplementing these sub-types with an engineering-psychological examination and examination of computers functioning in a network. Similar opinions are upheld by scientific and field personnel of the expert-criminalist divisions of the Ministry of Interior of the Russian Federation. Representatives of these divisions, V. Zubakha and A. Usov propose the following classification for computer-technical forensic examinations:[12] 1) computer hardware, 2) computer software, 3) information (data), and 4) computer network. These authors indicate that the last one should serve as complementary and be used only under certain conditions, whereas the first three types should be initiated by the investigator successively and used in combination when investigating crimes committed in the area of information technologies. V. Zubakha and A. Usov note that the first two types generally answer questions of diagnostic and classificatory nature concerning the identification of group dependency or specific equipment based on exceptional features. The third group (data examination), in their opinion, is one of the most important, seeing as 'answers to a lot of diagnostic and identification-related questions, associated with digital information, show the completeness of the entire evidentiary base'.[13] It should

9 Department of Informatics and Connections of Home Office of Republic of Lithuania. Data concerning criminal actions, committed during January–November 2009 [interactive]. [accessed 03-02-2010]. <http://www.vrm.lt/fileadmin/Image_Archive/IRD/Statistika/html_file.phtml?metai=2009&menuo=11&ff=1G&fnr=7>.

10 Rossinskaja, E. Sudebnaja ehkspertiza v ygolovnom, grazhdanskom i arbitrazhnom procese [Rossinskaja, E. Forensic examination in criminal, civil and arbitrate procedure]. Moskva, 1996, s. 31.

11 Kazancev, V. *Kriminalisticheskoe issledovanie sredstv kompjuternykh tekhnologij i programmnykh produktov* [Criminalistic examination of IT and software]. [interactive]. [accessed 03-02-2010]. <http://www.allpravo.ru/library/doc5195p0/instrum5196/item5201.html>.

12 Zubakha, V.; Usov, A. Vidovaja klassifikacija kompjuternoj–tekhnucheskoj ehkspertizy [Typological classification of computer-technical examinations]. *Ehkspertnaja praktika.* 2000, 48: 35.

13 Department of Informatics and Connections of Home Office of Republic of Lithuania. Data concerning criminal actions, committed during January–November 2009 [interactive]. [accessed 03-02-2010]. <http://www.vrm.lt/fileadmin/Image_Archive/IRD/Statistika/html_file.phtml?metai=2009&menuo=11&ff=1G&fnr=7>, p. 37.

be noted that there is no consensus on this issue, whether it is 'computer-technical', 'computer-technological', 'computer-forensic', 'forensic-cybernetic' or yet another type of examination that can subsequently be divided into several more types based on the object being examined.[14]

Polish researchers define 'computer examinations' as 'examinations related to the identification of computer hardware, determination of software and application configuration, searching for and reconstruction of information retained on computer data storage and other electronic documents'.[15]

In Lithuania, examinations of this type are called examinations of information technologies and are carried out by the Division of Information Technologies Examinations of the Forensic Science Centre of Lithuania under the Ministry of Justice of the Republic of Lithuania and in the Division of Information Technologies Investigation of the Lithuanian Police Forensic Science Centre. The first examination of this type, called 'computer examination' was carried out by the Forensic Science Centre of Lithuania (FSCL) in January 1995, in criminal case No. 20-2-207-94 concerning the embezzlement of GSK 'Šarkuva'.[16]

There is little interest among Lithuanian researchers in the potential of these examinations or their practical methodology. Nonetheless, P. Pošiūnas has reflected on these examinations back in 1994. In his classification of examinations performed in Lithuania, he initially defined them as 'engineering-technological examinations'[17], and eventually ascribed them to financial investigations as one of the 'new technical issues, associated in particular with the use of digital information when conducting financial investigations, seeing as financial operations and economic information are computerized in the majority of companies and organizations'.[18]

M. Strachinsky was one of the first to discuss the precise terms describing such examinations in his article. However, he did not provide any concise definition for such examinations either.[19] In our article, we will use the term 'criminal forensic examination of information technologies', because this particular term is most used in practice and,

---

14 See: Rossinskaja, E., *supra* note 10; Kazancev, V., *supra* note 11; Zubakha, V.; Usov, A., *supra* note 12; Semenov, V. *Sudebno-kiberneticheskaja ehspertiza – instrument borby c prestupnostju XXI veka* [Semenov, V. Forensic-cybernetic examination—a tool for fighting criminality in the twenty-first century]. Moskva: Konfident, 2001.

15 Computer and digital forensic examination of data mediums [interactiv] [accessed 03-02-2010]. <http://clk.policja.pl/portal/clk/408/10434/BADANIA_SPRZETU_KOMPUTEROWEGO_I_CYFROWYCH_NOSNIKOW_DANYCH.html>.

16 Stračinskij, M. Kompiuterinės ekspertizės Lietuvoje: teorinės bei praktinės problemos, tyrimų tendencijos ir perspektyvos [Computer examination in Lithuania: theoretical and practical problems, trends and prospects]. *Kriminalistika ir teismo ekspertizė: mokslas, studijos, praktika*. Vilnius: Mykolo Romerio universitetas, 2007, p. 216.

17 Pošiūnas, P. *Teismo ekspertizės pagrindai* [The basis of forensic examination]. Vilnius: Spauda, 1994, p. 22.

18 Pošiūnas, P. Lietuvos teismo ekspertizės instituto veiklos apžvalga ir perspektyvos. *Kriminalistikos ir teismo ekspertizės problemos. Mokslo darbų rinkinys* [Review and prospects of Lithuanian Forensic Examination Institute activity. Problems of criminalistic and forensic examination: selected studies]. Vilnius: LTEI, 1996, p. 12.

19 Stračinskij, M., *supra* note 16, p. 218.

in the authors' opinion, it best expresses the substance of such examinations. The term also encompasses the examination of computers themselves and other information devices, computer hardware as well as cellular telephones, or other devices operated with the help of information technology.

In evaluating the potential of criminal forensic examination of information technologies, it is important to define the objects being examined, and what methods are used by the experts when examining the objects submitted to them. The objects received for examination at the FSCL include:[20] a) computer hardware, b) computer data storage, c) computer systems—hardware, operating systems, software applications, data, d) password-unprotected pocket (handheld) computers, mobile telephones, digital photo cameras, e) payment cards.

The following methods are used during a criminal forensic examination of information technologies:[21] 1) retrieval of information from hard disk drives, floppy disks and other computer storage devices, such as Zip drives, Jaz drives, optical or compact disks, magnetic tapes, 2) retrieval of information from different operating systems on the computer, 3) reconstruction of deleted or corrupted information in data storage devices, 4) searching for documents or other information in computer data storage submitted for examination as well as in free areas of the disks, 5) collection of evidence from computer peripheral devices able to accumulate digital information—external hard disk drives, magnetic tape cassettes, etc., 6) determination of the operability of software, its part or technical accessory of the computer, 7) establishing the sequence of events occurring in the computer: whether a given event occurred prior to another given event, 8) determining the configuration of the computer hardware, 9) retrieval of information from password-unprotected pocket (handheld) computers, mobile telephones, digital photo cameras.

2. Problems in the Practice of Criminal Forensic Examination of Information Technologies

Criminal investigators generally request an examination of information technologies for the following reasons:[22]

- to retrieve information stored on an electronic computing device;
- to retrieve information stored on a mobile telephone;
- to retrieve information associated with an individual, organization or specific activity stored on an electronic computing device;

---

20 Jankauskas, V.; Kligys V. Informacinių technologijų ekspertizė Lietuvos teismo ekspertizės centre: dabartis ir perspektyvos [Information technology examinations at the Lithuanian Forensic Examination Centre: realities and prospects]. *Kriminalistika ir teismo ekspertizė: mokslas, studijos, praktika*. Vilnius: Mykolo Romerio universitetas, 2005, p. 9.

21 *Ibid*., p. 10.

22 Information Technology Examination Officer's Questionnaire [interactive]. [accessed 03-02-2010]. <http://www.fdic.gov/regulations/examinations/questionnaire/index.html>.

- to retrieve information from a password-protected file stored in a data storage device;
- to determine when information was last modified in a specific file;
- to determine whether any information pertaining to an individual, organization or specific activity has been deleted from an electronic computing device (or medium) submitted for examination. If yes, reconstruction of the found fragments is requested, if possible;
- to crack a password-protected system;
- to retrieve information pertaining to an individual, organization or specific activity stored in an electronic notebook;
- to identify the operator of a SIM card submitted for examination;
- to retrieve SMS messages (including deleted ones) stored on a SIM card;
- to identify the last base station of SIM card registration (this information being particularly relevant when much time has passed since the SIM card's last registration and the operator no longer has this information).

The authors of this article surveyed the majority of cyber crime officials involved in investigations of crimes on electronic data and information systems security. The results of the survey revealed that when requesting examination of evidence, officials rarely consult experts on the formulation of questions.

An expert or a specialist may have to deal with classification, diagnostics or identification tasks in the course of the investigation. For classification or diagnostic tasks, experts may invoke interdisciplinary or special methods used by other sciences (not criminalistics) such as programmatic-technical methods of informatics, computation technique, etc. However, when tackling tasks of identification, criminal forensic techniques of cognition are used exclusively—the method of criminal forensic identification. This method represents one of the techniques used to establish facts in a pre-trial investigation or court proceedings. It differs from identification used by other sciences and techniques in its very essence and the way that the results are presented. For the results of expert examinations to become truly relevant to a criminal investigation, it is necessary to adhere to the common provisions of criminal forensic identification theory: to define what the identification indications are; to classify these indications; to establish what the corpus thereof needs to be for a given conclusion and to observe the appropriate established procedure of examination. Analogous requirements exist for analyses of the diagnostic type.

However, practice shows that IT examiners lack the proper methodologies for this purpose. This is because the examination of each object is different and requires special knowledge and creativity. Nonetheless, this situation is a matter of concern, because in Lithuania, there are no prescribed methodologies for a criminal forensic examination of information technologies, either of general or specific nature. Approbation or practical application aspects are out of the question altogether.

Positive tendencies can also be observed in the activities of institutions carrying out the examination of information technologies. For example, the FSCL has undertaken the implementation of a quality control system according to the European Standard 17025.

The main efforts in this field include the preparation of quality guidelines and examination methods.[23] The Lithuanian Police Forensic Science Centre (LPFSC) has also been accredited according to this standard, while the quality management system is still under development. In December 2007, the LPFSC, in association with the European Public Law Centre in Greece, participated in a twinning project on the development of information technology examinations in Lithuania and the creation of standard operation procedures for the examination of information technologies.[24] Unfortunately, this is not enough.

Another problem in this field is that an overly small number of specialists are engaged in the examination of information technologies. For example, the FSCL has examinations performed by 9 experts. Meanwhile, there are only 3 specialists at the LPFSC. Examiners working directly in the LPFSC are impeded by the fact that they are simultaneously responsible for maintaining the computer equipment in the Centre. Examiners at the LPFSC must also formalize their conclusions in an examination protocol (in line with orders No. I-51 of 11 April 2003 and No. I-146 of 30 October 2007 of the Prosecutor General of the Republic of Lithuania). This paperwork takes from several hours to several days to complete. This enables the investigators to obtain answers faster; however, this stifles the performance of the examinations themselves.

The officials we surveyed indicate that they refer most such examinations to the LPFSC. It should be noted that lately, the LPFSC has focused on developing and applying new types of examinations (e.g., DNA analysis), and has thus overlooked other types of examinations, including those of information technology. Considering that IT examinations are carried out by two specialists only, their workloads tend to be overwhelming, and this prevents them from improving their qualification, attending training regularly organized by institutions of the European Union on the most advanced methods and technologies in the practice of such examinations. For example, mobile telephone examinations are practically not conducted at the LPFSC altogether. Experts working in Lithuania contend that 'examination of information technologies is a complicated and unrewarding task'. The head of the Division of Information Technologies Examination at the FSCL, V. Kligys noted that 'the mentioned examinations undoubtedly require state-of-the-art and costly equipment and software, which results in quite a headache for Lithuanian experts. It is also true that there are certain unique cases, where they might need 'tools' for examining technologically obsolete hardware or software that would be of use for that one specific case only.'[25] Experts indicate that the type of examination is

23 Juodkaitė-Granskienė, G. Lietuvos teismo ekspertizės centro raida. *Tarptautinės mokslinės praktinės konferencijos „Teismo ekspertizės raida: pasiekimai ir iššūkiai" mokslinių straipsnių rinkinys* [Development of Lithuanian Forensic Examination Centre. Proceedings of international conference 'development of forensic examination: achievement and challenges']. Vilnius: LTEC, 2005, p. 12.

24 Assoc. dr. E. Bilevičiūtė prepared and presented conclusion concerning conformity of standard procedures of IT examinations (8 documents) with the main legal acts of Lithuania regulating penal procedure and accomplishment of criminalistic examinations in project: *EU TWINNING PROJECT LT/2004/JH/01. Legal evaluation of the preparation and implementation of the Quality Assurance Programme within the LPFSC. Standard Operation Procedures legal compliance with the Lithuanian Legal System. – ACTIVITY 2.3*

25 Stračinskij, M., *supra* note 16, p. 217; Digital Forensic Investigation [interactive]. [accessed 03-02-2010].

determined by the objects submitted and the situation in which these objects were used for committing a criminal act. Moreover, constant improvements in information and communication technology lead to the broadening of the scope of questions presented to specialists and experts, making each examination highly individual by nature. They note that examinations are becoming increasingly more complex due to increasing volumes, the number of objects and the capacity of information storage devices submitted for examination.

The surveyed officials indicate yet another problem—the particularly long terms for carrying out examinations. Indeed, examinations of information technology may take up to 2 to 2.5 years. The examination itself takes from several days to several months; however, it takes up to 3 years for the investigators to receive the conclusions of the examinations due to very long queues. The main reason for such long terms is the particularly large volume of information that needs to be examined and analysed. The work of experts and specialists is in turn hindered by ever-increasing volumes of digital information stored in the media. For example, a survey of FSCL experts revealed that over the recent years, there were thousands of objects examine; however, the number of such examinations is estimated based on the number of digital objects examined and not objects received (one hard disk drive may contain around 250,000 objects that are to be examined). In comparison, the number of examined objects of non-digital format is slightly lower. Statistics reveal that over the last year, more than 1,000 objects have been examined (though the list of objects received for examination did not include objects of other types of examination, mostly documents). These numbers represent computers, computer system blocks, hard disks, CDs, DVDs, floppy disks, electronic notebooks, etc.

The method for calculating the number of objects examined at the LPFSC is the same as that for examinations of other types. Statistics are as follows: in 2005 there were 2 examinations and 6 objects, in 2006—3 examinations and 33 objects, in 2007—when they had 2 specialists working—9 examinations and 16 objects (computers, mobile telephones, CDs, DVDs and other objects), in 2008—12 examinations and 191 objects, in 2009—29 examinations and 74 objects. Files and megabytes are not counted as they are at the FSCL. Information technology examiners at the LPFSC conduct examinations, maintain all the computers, the computer network and the servers of the LPFSC, as well as engage in other work not related to examinations. The LPFSC last received equipment and software necessary for examinations in 2007; until then, the Centre carried out basic examinations only, not requiring complex software. However, the number of examinations has increased steadily with each year, thus amplifying the workload of the specialists.

Examination of digital information requires particular thoroughness on behalf of the experts. Therefore, subjective qualities of the individual who has mastered special knowledge remain among the key requirements ensuring the quality of such examinations.

<https://www.fox-it.com/en/fox-it-solutions/digital-forensic-investigation>.

Data obtained in our research indicates that the number of objects sent for examinations is rapidly increasing, as is the scope of examinations and volume of examination conclusions. It takes very long to have an examination carried out and to receive the specialist's conclusions. Based on the analysis presented in this article, pressing problems in the field of information technologies examinations in Lithuania should be urgently addressed by the following: an analysis of the key principles of the examinations' performance, introduction of technical-programmable systems for the attainment of tasks of examinations and specialists' conclusions, application of administrative competencies' enhancement methods, optimization of the problem-solving process, and reliance on scientific methods.

Conclusions

Crimes on electronic data and information systems security are detrimental to the functioning of information systems, the safety of important information and the interests of parties participating in the information activities, and those protected by the state. Investigation of crimes on electronic data and information systems security is impossible without the use of special knowledge. This entails the examination of information technologies.

In Lithuania, the examination of information technologies is performed by two institutions—the Lithuanian Police Forensic Science Centre and the Forensic Science Centre of Lithuania. Thus far, however, there are no prescribed and approved methodologies for criminal forensic examination of information technologies, either of general or specific nature. Very few specialists performing examinations work in these institutions. Moreover, specialists at the Lithuanian Police Forensic Science Centre, in addition to their expert duties, must maintain the Centre's computer equipment. The heavy workloads prevent them from improving their qualification and introducing new examination methods. The qualification of investigators dealing with crimes on electronic data and information systems security also needs improvement. For example, guidelines for investigators should be continuously published and updated. Lithuanian institutions should also use special information technology risk management programmes to prevent computer crimes.

References

Computer and digital forensic examination of data mediums [interactive]. [accessed 03-02-2010]. <http://clk.policja.pl/portal/clk/408/10434/BADANIA_SPRZETU_KOMPUTEROWEGO_I_CYFROWYCH_NOSNIKOW_DANYCH.html>.

Decision of Government of Republic of Lithuania of 2001 08 10, No. 984. *Official Gazette.* 2001, No. 71-2534.

Decision of Government of Republic of Lithuania of 2002 06 20, No 670. *Official Gazette.* 2005, No. 78-2823.

Department of Informatics and Connections of Home Office of Republic of Lithuania. Data concerning criminal actions, committed during January-November 2009 [interactive]. [accessed 03-02-2010]. <http://www.vrm.lt/fileadmin/Image_Archive/IRD/Statistika/html_file.phtml?metai=2009&menuo=11&ff=1G&fnr=7>.

Digital Forensic Investigation [interactive]. [accessed 03-02-2010]. <https://www.fox-it.com/en/fox-it-solutions/digital-forensic-investigation>.

Förster, Ch. Der polizeiliche Sachverständige IT-Forensik [Police IT examination-Forensic]. *Kriminalistik*. 2007, 61.

Information Technology Examination Officer's Questionnaire [interactive]. [accessed 03-02-2010]. <http://www.fdic.gov/regulations/examinations/questionnaire/index.html>.

Jankauskas, V.; Kligys, V. Informacinių technologijų ekspertizė Lietuvos teismo ekspertizės centre: dabartis ir perspektyvos [Information technology examinations at the IT in Lithuanian Forensic Examination Centre: realities and prospects]. *Kriminalistika ir teismo ekspertizė: mokslas, studijos, praktika*.Vilnius: Mykolo Romerio universitetas, 2005.

Juodkaitė-Granskienė, G. Lietuvos teismo ekspertizės centro raida. *Tarptautinės mokslinės praktinės konferencijos „Teismo ekspertizės raida: pasiekimai ir iššūkiai" mokslinių straipsnių rinkinys* [Development of Lithuanian Forensic Examination Centre. Proceedings of international conference 'Development of forensic examination: achievement and challenges']. Vilnius: LTEC, 2005.

Kazancev, V. *Kriminalisticheskoe issledovanie sredstv kompjuternykh tekhnologij i programmnykh produktov* [Criminalistic examination of IT and software]. [interactive]. [accessed 03-02-2010] <http://www.allpravo.ru/library/doc5195p0/instrum5196/item5201.html>.

Kažemikaitienė, E.; Bilevičienė, T. Problems of involvement of disabled persons in e-government. *Technological & Economic Development of Economy.* 2008, 14(2).

Law on changes and supplements of 13, 162, 191, 196, 197, 203, 206, 216, 219, 221, 309 articles and $198^{(1)}$ and $198^{(2)}$ articles of The Criminal Code of the Republic of Lithuania. *Official Gazette.* 2004, No. 25-760.

Law on changes and supplements of 7, 38, 47, 63, 66, 70, 75, 82, 93, 129, 166, 167, 172, 178, 180, 181, 182, 183, 184, 185, 189, 194, 196, 197, 198, $198^{(1)}$, $198^{(2)}$, 199, 202, 213, 214, 215, 225, 227, 228, 231, 233, 235, 252, 256, 257, 262, 284, 285, 312 articles and titles of XXVI, XXX chapters, supplement by $256^{(1)}$, $257^{(1)}$ articles of The Criminal Code of the Republic of Lithuania. *Official Gazette.* 2007, No.81-3309.

Pošiūnas, P. Lietuvos teismo ekspertizės instituto veiklos apžvalga ir perspektyvos. *Kriminalistikos ir teismo ekspertizės problemos*. *Mokslo darbų rinkinys* [Review and prospects of Lithuanian Forensic Examination Institute activity. Problems of criminalistic and forensic examination: selected studies]. Vilnius: LTEI, 1996.

Pošiūnas, P. *Teismo ekspertizės pagrindai* [The basis of forensic examination]. Vilnius: Spauda, 1994.

Rossinskaja, E. *Sudebnaja ehkspertiza v ygolovnom, grazhdanskom i arbitrazhnom procese* [Forensic examination in criminal, civil and arbitrate procedure]. Moskva, 1996.

Semenov, V. *Sudebno-kiberneticheskaja ehspertiza – instrument borby c prestupnostju XXI veka* [Forensic-cybernetic examination—a tool for fighting criminality in the twenty-first century]. Moskva: Konfident, 2001.

Stračinskij, M. Kompiuterinės ekspertizės Lietuvoje: teorinės bei praktinės problemos, tyrimų tendencijos ir perspektyvos [Computer examination in Lithuania: theoretical and practical problems, trends and prospects]. *Kriminalistika ir teismo ekspertizė: mokslas, studijos, praktika.* Vilnius: Mykolo Romerio universitetas, 2007.

The Criminal Code of the Republic of Lithuania. *Official Gazette*. 2000, No. 74 – 2262, with further amendments and supplements.

Usov, A. *Sydebno-ehspertnoe issledovanie kompjuternykh sredstv i sistem* [Forensic examination of computer tools and systems]. Moskva, 2003.

Zubakha, V.; Usov, A. Vidovaja klassifikacija kompjuternoj–tekhnucheskoj ehkspertizy [Typological classification of computer-technical examinations]. *Ehkspertnaja praktika.* 2000, 48.

INFORMACINIŲ TECHNOLOGIJŲ TYRIMŲ PANAUDOJIMAS TIRIANT NUSIKALTIMUS ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ SAUGUMUI

Lina Novikovienė, Eglė Bilevičiūtė

Mykolo Romerio universitetas, Lietuva

Santrauka. *Ilgalaikė Informacinių technologijų ir telekomunikacijų plėtotės strategija yra šalies ūkio ir informacinės visuomenės raidos procesų neatsiejama dalis, kurios tikslas – iš esmės pagreitinti valstybės ir visų ūkio veiklos sektorių valdymo darbų modernizavimą grindžiant jį informacinių technologijų ir telekomunikacijų priemonių naudojimu bei skatinti informacinių technologijų ir telekomunikacijų modernių produktų gamybą Lietuvos reikmėms ir eksportui. Atsiranda naujų verslo, viešojo administravimo, darbo, mokymosi ir kultūros plėtojimo galimybių. Ypatingą reikšmę įgyja informacija, žinios, kompetencija, gyventojų, verslininkų bei valdžios gebėjimas naudotis informacinių technologijų teikiamomis galimybėmis. Taip pat labai svarbus tampa gyventojų, verslo, visos visuomenės ir valstybės informacinis saugumas.*

Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui yra dažnas ir skaudus reiškinys Lietuvoje, tačiau jų tyrimas dėl kriminalistinių metodikų, darbuotojų ir kitų resursų trūkumo dažnai užtrunka gan ilgai, nėra apibendrinama ekspertinė praktika tokiose bylose, nekuriamos jos pagrindu ekspertinės profilaktinės priemonės. Autorių tyrimo pagrindinis tikslas išanalizavus specialiųjų žinių taikymo (informacinių technologijų kriminalistinių tyrimų) galimybes ir ypatumus, informaciją apie specialiųjų žinių panaudojimo

nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui tyrimo plėtros tendencijas, pateikti pasiūlymus dėl informacinį saugumą lemiančių kriminalistinių profilaktinių priemonių plėtros krypčių Lietuvoje. Straipsnyje pristatyta dalis tyrimo rezultatų, kitame straispnyje tęsdamos atlikto tyrimo rezultatų analizę, autorės pristatys ekspertinės profilaktikos ypatumus.

Kaip tyrimo šaltiniais buvo naudotasi nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui statistiniais duomenimis. Darbe buvo remtasi empiriniais duomenimis, kurie buvo gauti taikant ekspertinės apklausos metodą, apklausiant Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo valdybos nusikaltimų tyrėjus ir Lietuvos teismo ekspertizės centro bei Lietuvos policijos Kriminalistinių tyrimų centro informacinių technologijų tyrimus atliekančius ekspertus (specialistus).

***Reikšminiai žodžiai**: informacinių technologijų kriminalistinė ekspertizė (tyrimas), specialiųjų žinių panaudojimas tiriant nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui, nusikaltimų profilaktika, ekspertinė profilaktika, informacinis saugumas.*

Lina Novikovienė, Mykolo Romerio universiteto Teisės fakulteto Verslo teisės katedros docentė. Mokslinių tyrimų kryptys: vartotojų teisių apsauga, civilinė teisė, kriminalistika.

Lina Novikoviene, Mykolas Romeris University, Faculty of Law, Department of Business Law, associated professor. Research interests: protection of consumer rights, civil law, criminal investigation.

Eglė Bilevičiūtė, Mykolo Romerio universiteto Teisės fakulteto Administracinės teisės ir proceso katedros docentė. Mokslinių tyrimų kryptys: administracinė teisė, kriminalistika, mokslo ir studijų teisė, informacinių technologijų taikymas teisėje.

Egle Bileviciute, Mykolas Romeris University, Faculty of Law, Department of Administrative Law and Procedure, associated professor. Research interests: administrative law, criminal investigation, research and study law, application of IT in law.