General Theoretical Issues of Improving Private Forensic Methods In The Field Of Combat Against Cybercrime

Khamidov Bakhtiyor Khamidovich,
Tashkent State University of Law, Senior teacher of the department of Criminalistics and Forensic Examination. E-mail: bahtiyor1984bsj@mail.ru

Karimov Boburjon Zokirovich
Tashkent State University of Law, Lecturer of the department of Criminalistics and Forensic Examination
E-mail: bkillusion311@gmail.com

Topildieva Dilrabo Mirshokhidovna
Tashkent State University of Law, Lecturer of the department of Criminalistics and Forensic Examination
E-mail: d.topildieva@gmail.com

ABSTRACT

This article critically examines the problems and gaps that arise in national legislation and law enforcement practice in the fight against cybercrime. Scientifically grounded ways and means of their overcoming are theoretically analyzed. In this regard, proposals and recommendations were developed for the development of private criminology methodologies for the development of the theory of forensic science.

The article was prepared with the views of theorists and practitioners, as well as technical research which were based on scientific and practical research in the field of countering cybercrime.

The study analyzes a number of proprietary forensic methods that serve to improve the effectiveness of investigative actions in the fight against cybercrime. National legislation, investigative and judicial practice, international prominent practices were studied, and their achievements and drawbacks were substantiated on the basis of the author's conclusions. Based on this, the most favorable directions for combating these crimes in Uzbekistan were selected.

The article provides a systematic, legal, scientific and methodological analysis of problems in this area and the author's conclusions on this matter. At the same time, the role and importance of advanced foreign experience and international standards in improving national legislation and ensuring the implementation of the tasks set in the State Program are emphasized. In addition, the concepts of "electronic evidence" and "digital evidence" were scientifically analyzed. Their content and technical features are scientifically and theoretically substantiated.

Keywords:
Cybercrime, private forensic methodology, digital forensics, digital device, computer, information, electronic data, digital information.
Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

Introduction

The 21th century is a time of great discoveries and inventions! Today, the process of digitization is fully being carried out in all spheres of society around the world. In particular, it will not be a mistake if we say as what the development of the digital economy, navigation, telecommunications, electronic currency, the transition to digital forms of payment [1] is the fourth revolution in human history.

The introduction of digital technologies has led to the emergence of new information of forensic significance on the one hand, and the expansion of activities related to the recording, storage, processing and research of digital information on the other hand [2]. In particular, in practice, all research in forensic technology is carried out

through digital technologies. This situation allows digital technologies to become more widely used in forensic science and to develop the scientific and technical base of research [3].

Issues related to the development of private forensic methods are also reflected in the judicial sphere of our country. In particular, in accordance with the Decree No. PD-5635 of the President of the Republic of Uzbekistan on January 17, 2019, increasing the effectiveness of work to ensure information security of the country has risen to the level of public policy. According to it, the tasks are set to create a specialized laboratory "digital forensics", improve the service "UZCERT" for rapid response to information security incidents in the national cyberspace, prevention of cybercrime, as well as improve the system of training professionals in this field [4].

At the same time, according to the state program approved by the Decree No. PF-5953 of the President of the Republic of Uzbekistan on March 2, 2020, one of the main tasks is to develop a national strategy for cyber security for 2020-2023 and the draft law of the Republic of Uzbekistan "On Cyber Security" [5].

As a result of reforms in the fight against cybercrime, computer-technical examination laboratories were established in the Forensic Expertise Centre of the Ministry of Internal Affairs of the Republic of Uzbekistan and the Republican Forensic Examination Centre named after Kh. Suleymanova under the Ministry of Justice of the Republic of Uzbekistan [6]. In addition, the State Inspectorate for Information and Telecommunications of the Republic of Uzbekistan and the State Unitary Enterprise for Cyber Security are authorized to exercise state control over compliance with the requirements of legislation, regulations and state standards in the field [7].

Another condition for improving the private forensic methodology in the fight against cybercrime in Uzbekistan is the decision of the President of the Republic of Uzbekistan, dated October 5, 2020, on approval of the Strategy "Digital Uzbekistan - 2030" [8] by Decree No. PD-6079.

International experience shows that the development of the digital economy implies the introduction of new approaches to the regulation of social relations associated with the circulation of computer information [9]. In world practice, the digitalization of the economy has been confirmed by the increasing need to protect public and private computer information from criminal encroachment [10]. In other words, the majority of cybercrimes committed are in the countries which digital economies are developed. This, in turn, requires the strengthening of cyber security measures in the country.

Supplying cybersecurity in the country means that it is the activity aimed at protecting systems, networks and applications from cyber-attacks. The purpose of such cyber-attacks is usually to gain access, to modify or delete confidential information, extort money from users, or disrupt normal business processes [11].

These cases oblige investigators to protect public and private law objects from cyber-attacks. In this regard, improving the forensic support of investigative activities will allow for the timely detection and prevention of crimes.

Because cybercrime is transnational in nature, the investigation and disclosure of it requires urgency and international cooperation. In most cases, investigative actions and search operations deviate from the jurisdiction of one state. Sometimes, disputes between states are heard by international courts. In doing so, the criteria for collecting, verifying, storing and evaluating digital evidence are addressed in accordance with international standards. Therefore, the place and role of advanced foreign practices in the storage and evaluation of digital evidence is of fundamental importance.

Developed countries have a number of best practices for working with digital evidence in investigative and judicial practice. For example, in the United States NIST - National Institute of Standardsand Technology (2006) [12], NIJ -

National Institute of Justice (2001) [13], in the UK ASPO - Association of Chief Police Officers (2011) [14], INTERPOL - (2019) [15], DFRWS (2008), ISO-27037 standards are internationally recognized rules. The reliability and scientific validity of these practices ensure that cases are considered objectively.

In the law enforcement practice of our country, the issue of harmonization of these standards with national legislation is still delaying. These circumstances jeopardize Uzbekistan's participation in international courts (admissibility of evidence, winning the case, etc.).

Today, the collection, verification, storage and evaluation of digital evidence related to a criminal case in the pre-trial and trial stages is carried out using digital technologies. In this sense, researches accomplishing in a specific form of objective reality called “virtual space” are gradually displacing materialist dialectical methods of knowing criminal activity [16].

The lack of scientifically based rules for working with digital evidence in investigative activities, the inconsistency of existing rules with international standards indicates the need for a number of studies in law enforcement practice. Accordingly, the issue of improving the methodological support of investigative activities raises conceptual views and approaches to the development of private forensic methods in the field.

The emergence of theories about private forensic methodologies, on the one hand, serves to expand science, on the other hand, leads to the specialization of fields. As a result, the mechanisms of the case proof process will be improved. The effectiveness of crime detection and prevention activities will increase.

The first appearance of private forensic methods in the field can be associated with the introduction of "Digital Forensic". The term "digital forensic" was originally named as "electronic forensic" or "computer forensic." In recent years, the use of the term "criminology" in the name of the field in the use of specialized knowledge has increased. In particular, the theory includes a number of concepts such as "medical criminology", "linguistic criminology", "economic criminology" [17], "computer criminology", "electronic criminology" [18].

The term "digital criminology" is a relative translation of the word “digital forensic” in English. In practice, the literal translation of this compound does not make sense. Therefore, it can be assumed that the term is used conditionally. These cases are explained by the specificity of approaches in legal systems.

In our opinion, criminology as a science does not exist in the United States and most European countries. In these countries, forensic science (psychology, expertise, evidence theory, etc.) is organized as an independent course on crime detection and prevention, that is to say, the fields are narrowly specialized.

In the national legal system, forensics combines all the areas of knowledge needed to detect and prevent crime. Of course, each methodology has its own advantages and disadvantages in this regard.

The use of the term "criminology" in the name of the field is considered by some scholars to be correct, while others do not agree. In particular, according to E.R. Rossinsky, the science of criminology is unique! Science has its own subject, system, functions, object and laws. There is no need to change the name to develop it. However, in some sources, “digital criminology” is also recognized as a network of forensic science [20].

When it comes to private forensic methods, its technical features cannot be ignored. In this regard, A.A. Zaitsev and A.V. Smolin's view that changes in information technology have led to a qualitative expansion of various technical devices [21] is vital. These cases, in turn, contribute to the popularity of cybercrime [22].

V.V. Vekhov's research on the development of a private forensic methods is of particular importance. He argues that in order to accelerate the development of criminology on the basis of information technology, it is necessary to develop

an automated methodology for the investigation of certain types of crimes, as well as recommendations, methods and techniques for their use in preliminary investigations. Later, the scientist proposes to study the private forensic methods "Computer information, criminological research of means of their reprocessing and protection" in the following three areas:

1. Criminological research of computer information;

2. Criminological research of computer devices, information systems and information and telecommunications networks;

3. Use of computer information, their reprocessing and protection for criminological purposes.

According to V. Vekhov, this methodology is considered as a system of technical rules, methods, techniques and recommendations developed on the basis of scientific rules for the collection, study and use of computer information, its reprocessing and protection in order to detect, investigate and prevent crimes [24].

In his research, V. Vekhov puts forward the concept of "computer information". He argues that the use of electronic traces - electronic carriers and computer information of criminological significance in their memory - as evidence in the conduct of electronic criminal proceedings is a feature of a mass nature [25].

E.R. Rossinsky confesses that Vekhov's theory on private methodology was developed in a narrow way. According to him, this theory is one part of the "Theory of information and computer support of criminal activity." He also believes that the term "electronic criminology" was misused by V. Vekhov [26].

In our opinion, V. Vekhov used the term "electronic criminology" in order to technically substantiate his theory. In essence, any digital device is powered by electricity. Technically, this is true. However, in terms of sources (electric current, magnetic field), the call "electronic information" is relative. In fact, the source does not directly process the information, but creates the conditions for it. Therefore, it is not acceptable to take it as a common feature.

E.R. Rossinsky shows that his theory has a broad fundamental character. This theory covers general theoretical problems, and by solving them, the technical, tactical and methodological departments of criminology are improved, and a continuous, interactive interaction with forensic science, criminal procedural law and other procedural disciplines is ensured. He connects the subject "Theory of information and computer support of criminal activity" with the laws of occurrence, movement, collection, inspection and use of computer information in the detection and investigation of crimes, as well as in criminal, civil (including arbitration) and administrative proceedings [27].

In our opinion, there are certain shortcomings in E.R. Rossinsky's theory on private methodology. In particular, the issues of the storage and evaluation of digital evidence have been neglected in the theoretical rule. In fact, the main purpose of finding, obtaining, recording, storing, researching and using evidence in a criminal case is also to establish the principles of legality, reasonableness and fairness in the process of proof. In other words, if the evidence is not evaluated on the basis of these principles, their collection, storage, and verification (research) lose their significance.

In the foreign literature, the computer device is recognized only as a type of digital technology. Therefore, the concepts of "information-computer" and "computer information" put forward by E.R. Rossinsky and V.Vekhov can be considered inappropriate. The reason is that today new types of digital technologies (netbooks, laptops, mobile devices, iPads, tablets, etc. [28]) are expanding. Each of them has the ability to create, store and process information.

If we agree with the ideas put forward by E.R. Rossinsky and V.Vekhov, then we should also put into practice the concepts of "computer information", "laptop information", "network

information", "tablet information", "mobile information" and so on. Theoretically, these concepts are not wrong. However, in terms of scientific and practical effectiveness, it is expedient to identify a feature that is common to all types of information technology. After all, the theory determines the direction of the correct organization of practice.

Technically, any digital device has a processor. The processor receives and processes information through the numbers "0" and "1". Depending on the nature of the information, the processor transmits digital (electronic) information directly to the user or through specific copiers [29] (assembler). Thus, a common feature is the technical origin, processing, storage and use of digital information.

E.P. Ishenko puts forward the point which "one of the most promising areas for forensic scientists today is the study of electronic traces left by mobile phones, credit cards, magnetic travel documents, computers, flash drives and other media and the development of methods for their use in investigative activities." In our opinion, it can be assumed that the methodology proposed by E.P. Ishenko is in a very narrow range. This method does not specify the stages of collection, storage and evaluation of digital technologies and their traces. Therefore, it is impossible to fully agree with this opinion.

The methodology may vary, but the rules and methods should be simple and effective for the participants in the process in the first place. In other words, the legitimacy, safety, reliability (scientifically based), objective and fairness of the chosen method are the main requirements for the criteria for evaluating the evidence. At the same time, the results of the evidence evaluated during the investigation must be confirmed in court. That is, the results of the examination and evaluation of digital evidence by a judge, prosecutor, attorney, and expert must give the same value. Otherwise, the charge shall be settled in favour of the suspect or accused in accordance with the applicable procedure.

As noted above, in order to increase the effectiveness of reforms in the field of cyber security in the country, it is necessary, first of all, to improve the mechanisms of detection and prevention of crime. Research in this area serves to arm investigative activities with science-based methodologies.

Theoretically, the development of private forensic methods in the field is one of the least studied areas in Uzbekistan. In this regard, although some aspects of the field have been studied by criminological scientists of our country, but monographic research has hardly been conducted. These circumstances also lead to various procedural and tactical errors in law enforcement practice.

According to the results of scientific research, investigation and analysis of court materials, in order to fully ensure the cyber security environment in the country, timely detection and prevention of crimes, the practice of " criminological support of cybercrime" (hereinafter referred to as the methodology) is considered expedient.

The subject of this methodology includes the mechanism of pre-trial proceedings and the emergence of digital information relevant to the case during the trial, the laws of their collection, verification, storage and evaluation, software, tactical and methodological support.

The methodology consists of the following areas:

1. Scientific and theoretical bases of criminological support of cybercrime activities. This section studies the theoretical rules, laws related to the subject, object, system, tasks and functions, principles, methods, problems and prospects of development.

2. Criminological research of digital information, devices, systems and networks. This section analyses the digital evidence relevant to the case in civil, criminal, administrative, economic, arbitration courts, their traces or the occurrence of other information related to the case, the laws of their collection, verification, storage and

evaluation. This methodology applies to all areas. This is because the rules for collecting, verifying, storing and evaluating digital evidence apply equally in all areas. In this regard, uniform procedures and standards for the use of digital evidence in foreign practice have been established [30].

3. Tactical and methodological support in the fight against cybercrime. This section examines the organization of the investigation of cybercrime, the conduct and planning of investigative versions, the tactical rules of the investigation, as well as the algorithm of the investigation of each typical investigation situation, the rules of control and evaluation of operational results.

In short, the criminological support of cybercrime activities serves to fill gaps in investigative activities. This situation ensures the safety of participants in criminal proceedings, maximum protection of their rights and freedoms protected by law.

List of used literature.

[1] *Pastukhov P.S.* On the need for the development of computer criminology. 2019 https://urfac.ru/?p=1536

[2] *Rossinskaya E.R., Shamaev G.P.* New section of forensics: forensic investigation of computer tools and systems // BAIKAL RESEARCH JOURNAL, vol.6, No.1, 2015.

[3] *Kamalova G.G.* Digital technologies in forensic science: problems of legal regulation and organization of application. Economics and Law. Bulletin of the Udmurt University. 2019.Vol. 29, no. 2.180 P.

[4] Paragraph 237 of the State Program on the implementation of the Action Strategy for the five priority areas of development of the Republic of Uzbekistan for 2017-2021 in the "Year of Active Investment and Social Development".

[5] State Program for the implementation of the Action Strategy for the five priority areas of development of the Republic of Uzbekistan for 2017-2021 in the "Year of Science, Enlightenment and Digital Economy" approved by the Decree of the President of the Republic of Uzbekistan dated March 2, 2020 No PD-5953, 243, 244-paragraphs.

[6] Resolution of the President of the Republic of Uzbekistan dated January 17, 2019 No PR-4125 "On measures to further improve forensic activities."

[7] Resolution of the President of the Republic of Uzbekistan dated November 21, 2018 No PR-4024 on measures to control the introduction of information technology and communications, to improve the system of their protection.

[8] Decree of the President of the Republic of Uzbekistan No. PD-6079 of October 5, 2020 on approval of the Strategy "Digital Uzbekistan-2030" and measures for its effective implementation.

[9] *Linkov I., Trump B. D., PoinsatteJones K.* Governance Strategies for a Sustainable Digital World // Sustainability (Switzerland). 2018. Vol. 10. Iss. 2. URL: http://www.mdpi.com/2071-1050/10/2/440/htm; Ali M. A., Hoque M. R., Alam K. An Empirical Investigation of the Relationship Between E-Government Development and the Digital Economy: the Case of Asian Countries // Journal of Knowledge Management, 2018. Vol. 22. Iss. 5. URL: https://www.emeraldinsight.com/doi/abs/10.1108/JKM-10-2017-0477.

[10] *Dremlyuga R.I.* Computer information as a subject of encroachment with unauthorized access: a comparative analysis of US and Russian legislation. The study was carried out with the financial support of the Russian Foundation for Basic Research within the framework of scientific project No. 18-29-16129. https://cyberleninka.ru/article/n/kompyuternaya-informatsiya-kak-predmet-posyagatelstva-pri nepravomernom-

dostupe-sravnitelnyy-analiz-zakonodatelstva-ssha-i-rossii

[11] https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html

[12] Guide to Integrating Forensic Techniques // NIST Special Publication 80086.

[13] U.S. Department of Justice Office of Justice Programs National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. 2001.

[14] ACPO Good Practice Guide for Digital Evidence, Version 5 (October 2011).

[15] INTERPOL Global guidelines for digital forensics laboratories. 2019.

[16] *Alymov D.V., Levchenkova V.A.* The main directions of research in the field of new information technologies used in forensic science. Forensic science in the development of the information society (59th annual forensic readings) [Electronic resource]: a collection of articles of the International Scientific and Practical Conference. - Electronic text data (2.33 MB). - M.: Academy of Management of the Ministry of Internal Affairs of Russia, 2018.

[17] *Rossinskaya E.R.* Theory of information and computer support for criminological activity: concept, system, basic laws. // Criminology. Forensic activity. Operational-search activity. // Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2 (89) 2019 196 P.

[18] *Vekhov V.V.* Electronic criminalistics: concept and system // Criminalistics: topical issues of theory and practice: collection of articles. - Rostov., 2017.

[19] *Rossinskaya E.R.* Revision of the definition of the subject of criminalistics: the pros and cons // Library of criminalistics. Scientific Journal, №4, 2012.

[20] *Jones, Andrew* (2008). Creation of a digital forensics laboratory. Butterworth-Heinemann. p. 312. ISBN 978-1-85617-510-4. Digital Forensics - https://ru.qaz.wiki/wiki/Digital_forensics

[21] *Zaitsev A.A, Smolin A.V.* On some elements of the forensic characteristics of cybercrimes. https://cyberleninka.ru/article/n/o-nekotoryh-elementah-kriminalisticheskoi-harakteristiki-kiberprestuplenii/viewer

[22] *Kopyrin M. Yu., Zhurbenko A. M.* Some aspects of the investigation of crimes related to fraud on the Internet // Education. The science. Career: Sat. scientific. Art. Int. scientific method. conf. In 2 vols. Resp. ed. A. A. Gorokhov. - 2018. - P. 218–220.

[23] *Vekhov V.B.* Automated methods of crime investigation as a new direction in criminologic technology // News of the Tula State University. Economic and legal sciences. Issue 3. Part II. Legal sciences. Tula, 2016.

[24] *Vekhov V.B.* Electronic criminology: concept and system // Criminalistics: topical issues of theory and practice: collection of articles. works of participants. scientific-practical conf. - Rostov, 2017.

[25] *Vekhov V.B.* Criminologic doctrine of computer information and means of its processing: dis. Dr. jurid. sciences. Volgograd, 2008. - 8 p.

[26] *Rossinskaya E.R.* Revision of the definition of the subject of criminalistics: the pros and cons // Library of criminalistics. Scientific Journal, №4, 2012.

[27] *Rossinskaya E.R.* Information and computer support of criminologic activity as a private forensic theory // Voronezh criminalistic readings. - 2017. - No. 2 (19). - P. 168–176.

[28] https://www.quora.com/What-are-digital-devices

[29] *Alfred W. Aho, Monica S. Lam, Ravi Seti, Jeffrey D. Ullman*. Compilers: principles, technologies and tools. second edition. - M: ID Williams LLC. 2008. P-29. ISBN 978-5-8459-1349-4.

[30] Belize (2011). Electronic Evidence Act., India (2000). Information Technology Act., In Indonesia (2012). Government Regulation No. 82 // (2008). Law No. 11 of 2008 Concerning Electronic Information and Transactions; Malaysian (1950). Evidence Act.; In Singapore (2012). Evidence (Amendment) Act.; In Tanzania (1967) Evidence Act., (2007). Written Laws (Miscellaneous Amendments) Act., (2015). Electronic Transactions Act.; In the UK (2015). Federal Rules of Evidence.