ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

# Х А Б А Р Ш Ы С Ы

# ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

# THE BULLETIN

THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

PUBLISHED SINCE 1944

5

SEPTEMBER – OCTOBER 2019

ALMATY, NAS RK

*NAS RK is pleased to announce that Bulletin of NAS RK scientific journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of Bulletin of NAS RK in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential multidiscipline content to our community.*

*Қазақстан Республикасы Ұлттық ғылым академиясы "ҚР ҰҒА Хабаршысы" ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Web of Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабаршысының Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді мультидисциплинарлы контентке адалдығымызды білдіреді.*

*НАН РК сообщает, что научный журнал «Вестник НАН РК» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Вестника НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному мультидисциплинарному контенту для нашего сообщества.*

**«Қазақстан Республикасы Ұлттық ғылым академиясының Хабаршысы».**
**ISSN 2518-1467 (Online),**
**ISSN 1991-3494 (Print)**
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы»РҚБ (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж. берілген **№5551-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.
Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
http://www.bulletin-science.kz/index.php/en/

---



Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

**«Вестник Национальной академии наук Республики Казахстан».**
**ISSN 2518-1467 (Online),**
**ISSN 1991-3494 (Print)**
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

---



Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

**Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.**
**ISSN 2518-1467 (Online),**
**ISSN 1991-3494 (Print)**
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz /, http://bulletin-science.kz

---



Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

**BULLETIN** OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 5, Number 381 (2019), 6 – 14 **https://doi.org/10.32014/2019.2518-1467.117**

UDC 343.983.25
MRNTI 10.85.41

**L. P. Klimovich[1], V. V. Molokov[2]**

[1]Siberian federal university, Krasnoyarsk, Russia,
[2]Siberian Law Institute of Ministry of Internal Affairs of the Russian Federation, Krasnoyarsk, Russia.
E-mail: klimovichl@mail.ru, vvmolokov@mail.ru

# CYBERCRIME IN THE CONDITIONS OF THE DIGITAL ECONOMY AND THE NEW TENDENCIES IN THE FORENSIC ENQUIRY DEVELOPMENT

**Abstract.** The rationale of the article is contingent on the possible security threats afflicting the digital economy in the context of the cybercrime spreading. The authors emphasize the important role of the law enforcement agencies in the prevention and suppression of computer crimes, determine their priority tasks and propose the possible solutions to them. The research content touches upon the topical issues of the computer forensic analysis in the conditions of the digital economy development in the Russian Federation. The study focuses on the experts' tasks, problems of implementation and demand for various types of the computer forensics, taking into account the tendencies of the criminal attacks on information and telecommunication systems and the equipment. The article justifies the importance of conducting the comprehensive computer forensics in order to obtain the forensically relevant information when investigating crimes committed using the Internet. From the standpoint of the economy digitalization development analysis, the authors offer the options for the forensics practice improvement and organization of the training for the experts in the forensic units. From the standpoint of the economy digitalization development analysis, the authors suggest the solutions for the computer forensics practice improvement and organization of the training for the experts in the forensic units.

**Keywords:** digital economy, information security threats, cybercrime, computer forensics, forensic examination, professional training.

**Introduction.** The concept of the "digital economy" became up-to-date in Russia quite recently and is connected with the legislative initiatives of the President and the Government of the Russian Federation. The very idea of implementation of the transition to the digital economic relations deserves support and is the scientific and technical progress. Issues of development and implementation of digital technologies in the framework of international integration of the countries of the Eurasian Economic Union are updated in the work of N.V. Kushzhanova and Dashgin Mahammadli [9]. Problems as always lie in the task and solution implementation, as well as creation of the foundation for reliable and secure functioning of the electronic information. The security issues are usually discussed from the standpoint of possible risks and threats, and the ways of their prevention and elimination are developed. An important role in countering the threats to the "digital economy" development shall be played by the law enforcement agencies. Therefore, the main tasks are the prevention, disclosure and investigation of the cybercrime. Their successful solution is impossible without obtaining the forensically significant information.

V. V. Putin, the President of the Russian Federation, in his Address to the Federal Assembly dd December 1, 2016, outlined the necessity to launch a large-scale system program for the development of the digital economy – the Russian economy of a new technological generation. The information society development strategy in the Russian Federation as of 2017–2030 has consolidated such a definition of the digital economy: this is an "economic activity in which the key production factor is the digital data, large volume processing and usage of the analysis allow to increase significantly the efficiency of various types of production, technologies, equipment, storage, sale, delivery of goods and services compared to traditional business forms" (scl. p) c .4) [23].

In order to implement the new progressive direction of the country's economic development, the Government of the Russian Federation approved and accepted for execution of the Russian Federation Digital Economy Program [17]. The implementation of this Program involves the development of the following basic digital technologies: big data; neurotechnology and artificial intelligence; distributed registry systems; quantum technologies; new production technologies; industrial Internet; robotics components and sensorics; wireless technology; virtual and augmented reality technology. The development of the new digital technologies is an inevitable process of modernity, in which a personal life, economy and production are integrated in a single information space that originated with the advent of the World Wide Web. [4].

**Methods.** This study is based on a system-activity approach, which is considered by the authors as an organic unity of tasks arising from the investigative situation, tasks of crime investigation and expert tasks of forensic examinations aimed at studying the properties and state of the objects of expert research. Historical and monographic research methods used in the study of the transformation of the problems solved by forensic examinations, in terms of the complexity of the methods of committing crimes in the field of high technology.

**Statement of the problem.** Though being attractive, the new technologies provide the high functioning efficiency only if they are highly protected from the external and internal information threats. In this regard, it is obvious that the development of the "digital economy" as many other information progress achievements will undoubtedly be accompanied by the realization of information security threats and the cybercrime development [8, 11, 26].

The use of digital technologies in a single information space provides not only the opportunities for the incredible business development, integration of information flows, exchange of knowledge and technologies, but also becomes a platform for illegal acts, as well as a means of crime commitment.

Types of crimes committed with the use of the computer and telecommunication technologies are enshrined in Chapter 28 of the Criminal Code of the Russian Federation: unauthorized access to the computer information (article 272 of the Criminal Code), creation, use and distribution of malicious computer programs (article 273 of the Criminal Code of the Russian Federation), violation of the operation rules for the data storage media, processing or transmitting computer information and information and telecommunication networks (article 274 of the Criminal Code of the Russian Federation), unlawful impact on the critical information infrastructure of the Russian Federation (Article 274.1 of the Criminal Code, was introduced starting from the 1st of January, 2018).

According to official statistics, in 2018, 132733 crimes committed using computer and telecommunication technologies were detected, which is 12.7 percent more compared to the same period of the previous year. 87323 crimes were not solved, which is 13.4 percent more compared to 2017. This statistics indicate the insufficiently developed by law enforcement agencies practice of solving such crimes.

In the meantime, it is obvious that cybercrime extends beyond the listed crimes. Computer information and telecommunication technologies often become the tools and means of the crime commitment, and the object of the crime covers the social relations such as property relations (art. 159.3, 159.6 of the Criminal Code), relations in the sphere of economic activity (art. 171.2 of the Criminal Code, art. 174,174.1 of the Criminal Code, etc.), relations in the field of public health and public morality (articles 228-228.4, 234-234.1 of the Criminal Code), etc. Considering various types of crimes committed with the use of high technologies, we proceed from the generally accepted concept of their understanding not in the criminal law aspect, but in the forensic, which allows us to understand the methods of committing and concealing a crime and, accordingly, to develop methods for the detection and investigation of such crimes. [18,109-110], including using the capabilities of forensic examinations.

In this connection, it can be concluded that the digital economy relying on advances in the computer technology and information telecommunications and expanding its borders in all the areas of economic, financial, industrial, commercial economic activity and in the public administration sphere, shall constantly be exposed to various criminal attacks, demanding the development of the new and improvement of the existing mechanisms for the information security of the global digital systems and technologies. The law enforcement agencies will have to confront threats, solve and investigate the crimes in the new economic environment. At the same time, measures for such crime prevention and control become of great importance. [10].

The emerging circumstances require the solution of a number of tasks facing the law enforcement agencies:

1. Training of the specialists with the special technical expertise in the field of functioning of the computer equipment, information and network technologies.

2. Analysis of the effective cybercrime investigation practice materials, and on this basis the development of the new and improvement of the existing methods for the high-tech crime solving and investigating.

3. Improvement of the organizational and tactical measures to obtain forensically relevant information both when checking statements (reports) about the prepared or committed crime with the use of the computer information and telecommunication technologies, and in the process of such crime investigation.

4. Conducting of the research and forensic science practice implementation of the new conducting forensic examination methods that meet the needs of investigative practices in solving the problems of the criminal case investigation concerning the use of the modern digital technologies.

The first and the second tasks are currently being solved within the framework of the specialist training in the educational organizations of the Ministry of Internal Affairs of Russia, the Federal Security Service of Russia and other law enforcement agencies and conduction of the scientific and applied research commissioned by the law enforcement agencies. The third task requires, first of all, the improvement of the operational search activity methods and techniques; in practice, it is implemented in the course of the operational search activity conduction (computer information obtaining, withdrawal of the information from the technical communication channels, etc.). The fourth task is quite complicated, its solution is multifaceted: first, it is the technical modernization of the laboratory equipment and the technical complexes included in the existing forensic laboratory equipment; secondly, this is the solution to the task for the creation of the research and analytical departments (services), whose main function is the analysis of the existing expert practice of the new expert task solution and the development of the modern expert research techniques for various kinds (types) of forensic examinations; thirdly, this is a solution to the financing issue concerning the technical modernization of the expert laboratory equipment, as well as the expert personnel professional retraining.

**Results.** We shall consider in more detail the upcoming development directions of the individual kinds (types) of forensic enquiry performed in the forensic units of various law enforcement agencies.

Primary attention shall be paid to the computer forensics (CF) which plays a leading role in the search and study of forensically significant information within the investigation of crimes committed with the use of computer information and telecommunication technologies. [2]. First of all, this particular forensic enquiry requires the continuous improvement of the experts' professional training level in forensic units and the contemporary development of its material and technical base.

As it has been already specified above, the digital economy relying on advances in computer technologies and info-telecommunications will be subject to various criminal attacks, requiring the development of the new and improvement of the existing information security mechanisms for global digital systems and technologies. Computer forensics is assigned to the leading role not only in the search of forensically relevant information but also in the cybercrime prevention [7].

At present the following adopted classification of CF is based on the research providing the computer environment component [19]:

- hardware computer forensics;
- software computer forensics;
- information computer (data) forensics;
- computer network forensics.

Hardware computer forensics examines the technical (hardware) tools of the computer system. The subject of this forensics type are the facts and circumstances substantiated on the basis of the research of the computer hardware operation and functioning consistencies related to the crime commitment.

The computer forensics is designed for the forensic software study implementation. Its subject is the consistencies of the development (creation) and application (use) of the computer system software. The purpose of this enquiry is to study the functional purpose, characteristics, requirements, algorithm, current state of the software presented for the study.

Information computer forensics is the key type of CF as it allows to form holistically the evidence base by the final resolution of the majority of issues related to the computer information. The purpose of this type of enquiry is the search, detection, analysis and evaluation of the forensically significant information prepared by the user or generated (created) by the software in order to organize the information processes in a computer system.

Computer network forensics is based primarily on the functional purpose of the computer tools implementing some network information technology. The necessity to distinguish it in a separate type is associated with the development of Internet technologies and the requirement to use the specific expertise in order to combine the obtained objects and the information about them for the effective solution of the assigned expert tasks.

Let us consider in detail what CF types will be in demand within the global digitalization of economic relations.

The basis of the modern digital relations is the credit and banking organizations. The development of digital technologies in the credit and banking sector will undoubtedly be based on the large-scale expansion of the remote banking services (RBS). Generally, a bank card holder installs the bank mobile application to his smartphone or uses the Internet service. The client-banking applications of the legal entities are developing in parallel with mobile applications. The problem of RBS system cyber-attacks aimed primarily at mobile applications of users and ATMs, remains relevant for several years [1]. The implementation of such attacks is based on the distribution of malicious software exposing both software and hardware of the computer systems. In most cases the distribution channel of such malware is the Internet communications. Consequently, to investigate such crimes it is necessary to conduct a whole complex of CF ranging from the hardware computer to computer network forensics. Since the process of conducting of various CF types involves multisystem platforms that are diverse in their hardware, system and application software, it is necessary to use the modern computer tools and technologies that must be skillfully used. The list of the typical tasks requiring solutions in this case [24]:

– determination of the type (type, brand), properties of the hardware, as well as its technical and functional characteristics;

– identification and study of the functional properties, as well as software settings;

– determination of the program initial state (for example, within the initial installation) and identifying the possible changes;

– determination of the goals and conditions for changing the software properties and state (deliberate changing of some functions, configuration to the specific hardware environment, etc.), investigation into the implementation way of software changes (for example, the effect of a malicious program, the errors in the software environment, unauthorized access);

– determination of the actual state of information, finding out whether there are any deviations from the typical state of the CF objects (for example, whether there are any malicious inclusions, violation of the information integrity, etc.);

– determination of the mechanism and circumstances of the event (case), substantiation of separate stages (phases, fragments) of the event according to the available data carrier information or its copies (for example, preparation of several copies of a business letter and sending it by the fax software to different addresses);

– investigation into the causes of changes in the properties of a computer network (for example, organization of the access control levels; substantiation the fact of network operation mode violation; facts (traces) of using external (“alien”) software use, etc.).

In the case of crime investigation concerning RBS systems that have been attacked or destroyed by viruses, there can be two sides - the server part of the bank's information system and the client module at the user side. Consequently, the software and hardware of the user devices and the data center of the bank shall be subject to the computer forensics. At the same time, difficulties may occur on the server side, under the pretext of ensuring the confidentiality of the processed information. In this regard, a legislative resolution of this problem is required.

It is important to note that cybercrimes are often transnational in nature. In some cases, the servers for information processing and storage, as well as postal services, instant messengers and social networks belong to the foreign companies and are deployed in other states. The ability to withdraw and study the electronic information placed in other states is the key to successful criminal exposure. At present, there is no clear mechanism for prompt obtaining of the information being interesting to the law enforcement agencies outside of the home state. In accordance with the criminal procedure legislation of the Russian Federation, the specified needs of the law enforcement agencies are met by directing of the legal assistance requests to other states. The deadlines for the execution of such requests are often longer than one year and are unacceptable to ensure the prompt investigation of a cybercrime. Thus, it is necessary to develop intergovernmentally a clear algorithm of international assistance in solving of the analyzed category crimes. The assistance terms and mechanisms, the specific responsibilities of the parties should be specified in this algorithm.

The following forensic information can be obtained from the subscriber devices in case of the fraud in RBS systems [5]:

- the traces of malicious software such as Trojan horse viruses or their signatures themselves;
- logs of the operating system and application software;
- crypto containers, password files;
- configuration files and scripts.

The economy digitalization develops the sphere of Internet application services for its support and operation, which means that the user is tasked with the skillful use of authentication tools (credentials, tokens, passwords, crypto containers, etc.). Many objects of economic relations are virtualized and, respectively, exist only in electronic form. The user identity leakage is a current and future time issue. And in this case, CF is crucial to obtain the material evidence. The issues and tasks facing the expert are approximately the same as the ones within the investigation of crimes with the use of RBS. The study of facts and circumstances in this area is a multi-step process as the computer-network forensics may require the hardware computer, the software computer, and, of course, the information computer forensics

Due to the large-scale use of the cryptographic security tools, it shall be necessary to apply the special knowledge in the related fields of mathematics and the computer system security. There may be difficulties due to the remoteness of the object of the forensic enquiry and the impossibility to obtain it for research. Intrinsically, it is difficult to assume the withdrawal of a large data center server or "mirroring" of the entire array of the information located on it.

This kind of computer forensics require various expertise to be more focused on Internet technologies and their development tools. Objects and facts in this case can serve as an evidence base only if they are connected in a chain of transactions accomplished with or without the user's actions on the network data processing devices.

The development of the digital economy in Russia is impossible without the global trends in the growth of the blockchain technology popularity [16]. And this is not only a cryptocurrency, in fact, it is a mechanism of a decentralized, secure and fault-tolerant registry. The scope of implementation is extensive - these are the financial transactions, securities registers, electronic commerce, logistics, etc [15]. The blockchain has proven its effectiveness and reliability in the experience of operations with the cryptocurrencies. The vulnerability of the blockchain technology lies only in the need to confirm transaction operations with private keys. Due to the complexity of the key, its storage is allowed both electronically and in paper form. The evidence from practice shows that the owners themselves are culpable of stealing keys or the vulnerabilities are discovered in the exchange security [6]. Thus, the software computer and information computer forensics can be used in the process of the blockchain technology crime investigation to determine the possible malicious software use, as well as to analyze the application event and the operating system logs.

However, the blockchain technology admits the unauthorized use of the remote computers' resources for cryptocurrency mining. As a rule, the organization of such botnets is based on the exploitation of any operating system vulnerabilities and the usage of the remote computer power for the benefit of unknown persons. In this type of the computer crime it is necessary to exclude the malware presence in the computer. In this case the software computer and the computer network forensics are demanded. The problematic issues of research of objects located in remote computer systems are updated in their research by D.A. Tarasov [25].

The cryptocurrency exchange hacking cases are frequent in the world practice [13]. The main vulnerability lies in the errors of configuration, administration and the site development security systems. The software computer and the information computer forensics of the server equipment is important in the investigation of such incidents. It is necessary to examine the event and security logs, as well as the configuration files.

The growing trend of the digital economy should be the growing popularity of the Internet of things [12]. Due to the large number of the "smart" equipment manufacturers, there is an increasing risk that developers do not pay enough attention to the security issues of the management services, the application software and the hardware configuration [3]. Thus, in order to search for crime traces, the investigation should include both the hardware and the software of the device along with the network configuration. All this shall require the appointment of a full range of the computer forensics. The role of forensic computer-technical expertise in solving complex expert problems is considered in [27].

The processes of the digital technology widespread use are already being actively implemented in the business, the economic and financial management sphere, the accounting automation has already been spread greatly simplifying the processing of accounting information large amounts and reporting. The new procedure for using cash registers is being introduced into practice, which provides the online transfer of the information about each calculation made in an organization to the server of the RF Tax Service. As already specified above, the development of digital technologies within the implementation of the credit and banking operations is based on a large-scale expansion of the remote banking services.

Electronic document management, modern technologies for creating a primary or other document, the use of automated accounting information processing systems - all these are the realities of the modern world, on the one hand, optimize lots of financial and business processes and are aimed at strengthening of the state control over the financial flow implementation. But, on the other hand, unfortunately, the digitalization of the economy gives rise to the new criminal schemes for money embezzlement, as well as the schemes for criminal proceeds introduction into the legal economic circulation.

The forensic economical examination is of great importance in obtaining the evidentiary information in the course of the investigation of such criminal cases. Specific objects of research in such expertise are the material storage media containing information on accounting and economic transactions relating to the subject of a specific examination. Such information can be provided for examination both on paper and on non-rewritable CD-R (DVD-R, BD-R) discs. In conditions when the compulsory paper media duplication of the accounting information is not required by the law [14], and the accounting data bases of an economic entity may be remotely accessible, it becomes necessary to obtain and withdraw such electronic information with the participation of a specialist (Articles 182, 183 of the Criminal Procedure Code). The need for the participation of a specialist in the field of forensic computer-technical expertise in the production of forensic economic examinations is updated in his works by A.I. Semikalenova and M.G. Nersesyan [20, 21]. The information withdrawn in electronic form is subsequently sent for examination. In such situations the practice of the last 5-7 years follows the path of the complex computer and economic forensics, when it is first necessary to decipher information in the electronic form and to convert it into the ordinary accounting and economic information and then it is to be analyzed by an expert economist.

Taking into account the ever-increasing volumes of the accounting information submitted in the digital form for the economic forensics, the development of the analytical software algorithms for the typical expert task solution will be required in the coming years. This will require, firstly, the analysis of the already existing positive practice of the typical EF expert task solution and, on this basis the development of software algorithms that make it easier for the expert to perform computations and calculations. Accordingly, the workplace of each forensic economist should be equipped with the

appropriate software and hardware to optimize the time of the enquiry. Secondly, it will be necessary to organize the retraining and the advanced training of the forensic economists in this direction.

**Conclusion.** Summarizing the issue of the development trends for the individual forensic examination kinds (types) in the context of the active digital technologies implementation in the economy, the public administration sphere in the Russian Federation and the resulting threats to information security and the cybercrime spread, the general conclusions shall be drawn.

First, the dominant role in the search and study of evidentiary information in the investigation of the computer and telecommunication technology criminal cases shall belong to the computer forensics. The solution of individual investigation tasks for such crimes shall require the development of the comprehensive forensic enquiry conducted in conjunction with the computer forensics. For example, the investigation of criminal cases related to the criminal proceeds legalization using the blockchain technology, through the implementation of the credit and banking operations, shall require the development of the new directions in the expert problem solution of the comprehensive computer and economic forensics.

Secondly, the relevant direction is the improvement of educational programs for the future investigators aimed at introducing of a special discipline - let's call it, for example, “Basics of the forensic computer knowledge”, giving an in-depth study of the functioning of the computer equipment, information and network technologies and possible directions of the criminal use of such technologies and their detection mechanism. In the same direction, in the coming years, the professional retraining and advanced training of the current employees of the forensic law enforcement units shall be required.

The search for new directions in the development of forensic enquiry in the conditions of the digital technology progress and thus, the possible criminalization of economic operations, is becoming a relevant area of the scientific research today.

**Л. П. Климович[1], В. В. Молоков[2]**

[1]Сібір федеральді университеті, Красноярск, Ресей,
[2]Ресей Федерациясы Ішкі істер Министрлігінің Сібір заң институты, Красноярск, Ресей

## ЦИФРЛЫҚ ЭКОНОМИКАДАҒЫ КИБЕРҚЫЛМЫС ЖӘНЕ СОТТЫҚ САРАПТАМА ДАМУЫНДАҒЫ ЖАҢА ТЕНДЕНЦИЯЛАР

**Л. П. Климович[1], В. В. Молоков[2]**

[1]Сибирский федеральный университет, Красноярск, Россия,
[2]Сибирский юридический институт Министерства внутренних дел Российской Федерации, Красноярск, Россия

## КИБЕРПРЕСТУПНОСТЬ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ И НОВЫЕ ТЕНДЕНЦИИ В РАЗВИТИИ СУДЕБНЫХ ЭКСПЕРТИЗ

**Аннотация.** Актуальность статьи обусловлена возможными угрозами безопасности, стоящими перед цифровой экономикой в условиях распространения киберпреступности. Отмечается важная роль правоохранительных органов в профилактике и пресечении компьютерных преступлений, определяются стоящие перед ними приоритетные задачи и предлагаются варианты их решения. Основное содержание работы затрагивает актуальные вопросы проведения судебных компьютерно-технических экспертиз в условиях развития цифровой экономики в Российской Федерации. Обсуждаются стоящие перед экспертами задачи, проблемы реализации и востребованность различных видов компьютерно-технических экспертиз с учетом тенденций преступных посягательств на инфотелекоммуникационные системы и оборудование. Обосновывается важность проведения комплексной компьютерно-технической экспертизы с целью получения криминалистически значимой информации при расследовании преступлений, совершаемых с использованием сети Интернет. С позиций анализа развития цифровизации экономики предлагаются варианты совершенствования практики проведения компьютерно-технических экспертиз и организации подготовки специалистов экспертно-криминалистических подразделений.

**Ключевые слова:** цифровая экономика, угрозы информационной безопасности, киберпреступность, судебная компьютерно-техническая экспертиза, профессиональная подготовка.

**Information about authors:**

Klimovich L. P., Doctor of Juridical Sciences, Associate Professor, Siberian federal university, Krasnoyarsk, Russia; klimovichl@mail.ru; https://orcid.org/0000-0001-5044-8397

Molokov V. V., Candidate of Engineering Sciences, Associate Professor, Siberian Law Institute of Ministry of Internal, Krasnoyarsk, Russia; vvmolokov@mail.ru; https://orcid.org/0000-0002-8901-6337

## REFERENCES

[1] Current Cyber Threats – 2017: Trends and Expectations (**2017**) // In Positive Technologies, available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (in Rus.).

[2] Andrew Jones, Stilianos Vidalis (**2019**). Rethinking Digital Forensics // Annals of Emerging Technologies in Computing. 2019. 3(2). P. 41-53. DOI: 10.33166/AETiC.2019.02.005 (in Eng.).

[3] Anti-virus report for 2017: let's forget about the malicious software (**2017**). Available at: https://habr.com/company/panda/blog/347430 (in Rus.).

[4] Bukht R., Heeks R. (**2018**). Defining, Conceptualising and Measuring the Digital Economy // International Organisations Research Journal. Vol. 13, N 2. P. 143-172. DOI: 10.17323/1996-7845-2018-02-07 (in Rus.).

[5] Imam Riadi, Sunardi, Muhamad Ermansyah Rauli (**2018**). Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics // Jurnal Teknik Elektro. 2018. 10(1): 18-22. DOI: https://journal.unnes.ac.id/nju/index.php/jte/article/view/14070/7872 (in Eng.).

[6] How bitcoins can be stolen: five most widespread ways (**2017**). Available at: https://coinspot.io/technology/bezopasnost/kak-kradut-bitcoiny-pyat-rasprostranyonnyh-sposobov (in Rus.).

[7] Khatuntsev N.A. (**2017**). Standardization of Terms and Definitions in Computer Forensic Science // Theory and Practice of Forensic Science. 2017. 12(4): 34-36. DOI: https://doi.org/10.30764/1819-2785-2017-12-4-34-36 (In Rus.).

[8] Kopczewski M., Napieralska A. (**2018**) Cyber space – risks to children and young people – research results // Scientific Journal of the Military University of Land Forces. Vol. 50, N 4(190). P. 45-58. DOI: http://dx.doi.org/10.5604/01.3001.0013.0720 (in Eng.).

[9] Kushzhanov N.V., Dashqin Mahammadli (**2019**). Cifrovaya povestka EAES…// Bulletin of National academy of sciences of the Republic of Kazakhstan. ISSN 1991-3494. 2019. Vol. 2. N 378. 55-61. https://doi.org/10.32014/2018.2518-1467.40 (in Eng.).

[10] Magdalena El Ghamari (**2018**). Cyberspace Protection – the Challenge of Our Time? // Bezpieczeństwo i Technika Pożarnicza. 2018. 49(1): 24-33 DOI: 10.12845/bitp.49.1.2018.2 (in Eng.).

[11] Makhalin V.N., Makhalina O.M. (**2018**). Management of calls and threats in digital economy of Russia // Upravlenie. 2018. 6(2). 57-60. DOI: https://doi.org/10.26425/2309-3633-2018-2-57-60 (In Rus.).

[12] Md Arafatur Rahman, A. Taufiq Asyhari. (**2019**). The Emergence of Internet of Things (IoT): Connecting Anything, Anywhere // Computers. 2019. 8(2):40. DOI: 10.3390/computers8020040 (in Eng.).

[13] The most explosive hacking attacks on cryptocurrency exchanges in 2017 (**2017**) // In Rossiiskii biznes on-line [Russian Business online], available at: http://www.innov.ru/news/it/nazvany-samye-gromkie-kha. (in Rus.).

[14] About the Accounting: the Federal Law № 402-FZ of December 4, 2011, articles 9, 10 (**2011**). (in Rus.).

[15] Pavlova Kristina I. (**2019**) The Advantages and Risks of Using Cryptocurrency in the Modern Digital Economy // Bìznes Inform. 2018. 7(486). 229-233. DOI: http://www.business-inform.net/export_pdf/business-inform-2018-7_0-pages-229_233.pdf (in Rus.).

[16] Prateek Goorha (**2019**). The Contractual Cryptoeconomy: An Arrow of Time for Economics // The Journal of The British Blockchain Association. 2019. 2(1):1-9. DOI: 10.31585/jbba-2-2-(1)2019 (in Eng.).

[17] "The Digital Economy of the Russian Federation." Program: approved by the RF Government Decree of July 28, 2017 (**2017**). N 1632-r. (in Rus.).

[18] Rossinskaya E.R. (**2016**) K voprosu o chastnoj teorii informacionno-komp'yuternogo obespecheniya kriminalisticheskoj deyatel'nosti // Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki. Izdatel'stvo: Tul'skij gosudarstvennyj universitet (Tula) ISSN: 2071-6184. 2016. N 3-2. P. 109-117 (in Rus.).

[19] Rossinskaia E.R. (**2011**). Forensic Enquiry in the Civil, Arbitral, Administrative and the Criminal Proceeding: Research and Practice Workbook. Moscow: Norma (in Rus.).

[20] Semikalenova A.I., Nersesyan M.G. **(2013)** Osobennosti uchastiya specialista v oblasti sudebnoj komp'yuterno-tekhnicheskoj ekspertizy v proizvodstve sudebno-ekonomicheskoj ekspertizy // Teoriya i praktika sudebnoj ekspertizy v sovremennyh usloviyah: materialy 4-j Mezhdunarodnoj nauchno-prakticheskoj konferencii. ISBN: 978-5-392-10099-6. M.: Prospekt, 2013. P. 251-253 (in Rus.).

[21] Semikalenova A.I., Nersesyan M.G. **(2011)** Problemy proizvodstva sudebnyh finansovo-ekonomicheskih ekspertiz, ob"ektom kotoryh vystupayut programmnye produkty avtomatizacii buhgalterskogo i finansovogo ucheta // Teoriya i praktika sudebnoj ekspertizy. Izd-vo: Rossijskij Federal'nyj centr sudebnoj ekspertizy pri Ministerstve yusticii Rossijskoj Federacii (Moskva). ISSN: 1819-2785 eISSN: 2587-7275. 2011. P. 128-132 (in Rus.).

[22] The Criminal Situation in Russia as of January – December. (2018). Available at: https://мвд.рф/reports/item/16053092/ (in Rus.).

[23] The Strategy of the Information-oriented Society Development in the Russian Federation as of 2017-2030: approved by the Decree of the Russian Federation President of May 9, **2017**. N 203 (in Rus.).

[24] Sudebnye ekspertizy v grazhdanskom sudoproizvodstve: organizaciya i praktika: nauchno-prakticheskoe posobie (**2014**) // Glava 8. Sudebnaya komp'yuterno-tekhnicheskaya ekspertiza / Pod. red. prof. E. R. Rossinskoj. M.: Izdatel'stvo YUrajt; ID Yurajt. ISBN 978-5-9916-4579-9 (Izdatel'stvo Yurajt). ISBN 978-5-9692-1569-6 (ID Yurajt). 2014: 364-384 (in Rus.).

[25] Tarasov D.A. (**2019**) Situacionnaya ekspertiza obstoyatel'stv formirovaniya sledovoj kartiny v komp'yuternyh sistemah // Ugolovnoe sudoproizvodstvo: problemy teorii i praktiki. Izdatel'stvo: OOO "Izdatel'stvo "YUniti-Dana" (Moskva). ISSN: 2346-8335. 2019. 1: 141-143 (in Rus.).

[26] Udalov D.V. (**2018**). Threats and Challenges of the Digital Economy // Economic security and quality. 2018. 1 (30). P. 12-17 (in Rus.).

[27] Usov A.I., Edzhubov L.G., Karpuhina E.S., Hatuncev N.A. (**2011**) Rol' komp'yuterno-tekhnicheskoj ekspertizy pri reshenii kompleksnyh zadach // Ekspert-kriminalist Izdatel'stvo: Izdatel'skaya gruppa "Yurist" (Moskva). ISSN: 2072-442X. 2011. 4: 31-35 (in Rus.).

## Publication Ethics and Publication Malpractice
### in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

**ISSN 2518-1467 (Online), ISSN 1991-3494 (Print)**

http://www.bulletin-science.kz/index.php/en/

Редакторы *М. С. Ахметова, Т. М. Апендиев, Д. С. Аленов*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 10.10.2019.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
13,9 п.л. Тираж 500. Заказ 5.