

Зарипов Азат Маратович,
студент,
Уфимский университет науки и технологий,
Уфа, Россия

Вахитова Гузель Валериевна,
кандидат филологических наук , доцент кафедры международного и
интеграционного права Института Права УУНиТ, Уфа, Россия

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация: *Статья посвящена анализу процессуально-криминалистических особенностей расследования киберпреступлений. Рассмотрены специфические особенности этого вида преступной деятельности, включая транснациональный характер, анонимность субъектов, использование шифрования и быстрое изменение цифровых следов. Особое внимание уделено проблемам организации первоначальных следственных действий, изъятия и экспертизы электронных доказательств, а также необходимости межведомственного и международного сотрудничества. В работе обосновывается необходимость адаптации традиционных следственных методов к реалиям цифровой среды и формулируются основные направления совершенствования деятельности правоохранительных органов в этой области. Результаты исследования могут быть использованы для оптимизации процесса сбора доказательств по уголовным делам о преступлениях в сфере информационных технологий.*

Ключевые слова: *киберпреступление, расследование, электронные доказательства, цифровые следы, кибербезопасность, компьютерная и техническая экспертиза, сетевые технологии, процессуальные особенности.*

Zaripov Azat Maratovich,
Student,
Federal State Budgetary Educational Institution of Higher Education
Ufa University of Science and Technology, Ufa, Russia

Vakhitova Guzel Valerievna,
Candidate of Philological Sciences, Assistant Professor of the Chair of the
International and Integration Law of the Institute of Law of the UUST

FEATURES OF INVESTIGATION OF CYBERCRIME

***Abstract:** The article is devoted to the analysis of the procedural and criminalistic features of the investigation of cybercrimes. The specific features of this type of criminal activity are considered, including the transnational nature, the anonymity of the subjects, the use of encryption and the rapid change of digital footprints. Special attention is paid to the problems of organizing initial investigative actions, seizing and examining electronic evidence, as well as the need for interdepartmental and international cooperation. The paper substantiates the need to adapt traditional investigative techniques to the realities of the digital environment and formulates the main directions for improving the activities of law enforcement agencies in this area. The results of the study can be used to optimize the evidence process in criminal cases of crimes in the field of information technology.*

***Keywords:** cybercrime, investigation, electronic evidence, digital traces, cybersecurity, computer and technical expertise, network technologies, procedural features.*

The penetration of digital technologies into all spheres of public life has led to the emergence of a qualitatively new criminal environment in which traditional investigative methods often prove ineffective. Cybercrimes require a systematic

review of the existing procedural and criminalistic approaches of law enforcement agencies. The investigation of such offenses is hampered by their international nature, the anonymity of intruders, the use of sophisticated encryption methods, as well as the high rate of change in digital footprints. The development of the IT sector and the constant introduction of network tools into everyday life have contributed to the emergence of new forms of illegal activity using electronic devices, which necessitated the creation and improvement of specialized methods for detecting and investigating information crimes. According to Interior Minister V.A. Kolokoltsev, compared with 2023, the number of crimes involving the use of information and telecommunication technologies increased almost 16 times — an increase of 92 percent[4]. The specifics of certain types of such crimes are due to the fact that some of them are directly regulated by the provisions of Chapter 28 of the Criminal Code of the Russian Federation[1], while responsibility for others is fixed by specialized regulations. Illegal actions in the field of computer technology cover a wide range of actions performed using various electronic devices and software and hardware complexes.

There is no well-established definition of the concepts of "cybercrime" and "computer information crime" in the scientific community. Thus, D. N. Karpova considers cybercrime as a socially dangerous act aimed at causing economic or political damage or undermining the ethical foundations of an individual or organization using Internet technologies [6, p. 47]. Although this interpretation is not generally accepted in criminology and criminal procedure law, it is distinguished by its substantial completeness - the key features of this phenomenon are highlighted here. An example is the identification of the illegal use of information technology in the financial sector when investigating the activities of some club establishments: cases of profit from gambling through a network outside special permitted territories have been established [3, p. 246].

One of the most common types of cybercrimes remains phishing, a type of fraud whose main purpose is to seize personal data (for example, bank details or

account numbers) for the subsequent theft of funds from citizens [8, p. 99]. When analyzing crimes of this kind, it is necessary to pay special attention to the importance of various legal mechanisms for obtaining information about the details of the incident.

A characteristic feature of such cases is the almost complete absence of voluntary confessions on the part of suspects or accused; this is due to the careful preparation of criminals and awareness of their actions — often the perpetrators are confident that it is impossible to bring to justice or consider their actions legitimate.

During the investigative measures, it is necessary to establish key circumstances: firstly, to confirm the illegality of the committed act; secondly, to determine the object of the encroachment (given the development of the digital space, it may not only be about information); further, to fix the place of commission of the illegal act and its consequences; to find out how to implement criminal intentions and the role of the technical means used; identify the elements of a crime.

Competent recording of digital traces of illegal activities and their correct removal are necessary conditions for a comprehensive investigation of criminal cases in this category. As an example, the following episode can be cited: citizen T., having found on the Internet an offer to deposit funds at interest to account No. 890470*, opened through the Visa Qiwi Wallet service, made a money transfer; subsequently, access to these funds was blocked [4, p. 230].

During the investigation of criminal cases, the investigator analyzes the collected factual data in order to build a logically coherent system of relationships between events, identify their dependencies and reasonably formulate conclusions. Such work is aimed at step-by-step establishment of the circumstances of the case and proof of the role of suspects in the commission of criminal acts. The evidence base is formed through a set of operational search, investigative and other

procedural actions in relation to specific crimes.; The methods of these activities are fixed by law, but are not limited to the above list.

A key factor in the success of the investigation is the high level of professional competence of the specialist directly leading the case. At the same time, one of the serious problems of such investigations is the lack of technical training of law enforcement officers: many of them have specialized legal education, but do not have special knowledge in the field of information technology. The lack of IT competencies significantly complicates a comprehensive understanding of the features of digital incidents and prevents a correct assessment of their characteristics, which negatively affects the objectivity of perception of the incident picture.

In the context of this study, it is advisable to consider the specifics of cybercrimes involving military facilities. Despite the fact that military infrastructure rarely becomes the main target of cyber attacks, the information systems of the Armed Forces of the Russian Federation attract the attention of intruders by the presence of strategically important data. An example is the 2022 incident involving the distribution of malicious WannaCry software against the resources of the Ministry of Defense of the Russian Federation; according to TASS[10], these attempts were neutralized in a timely manner. Official reports on attacks on the IT infrastructure of field units of the Russian army are rarely published due to the specifics of government policy to ensure the security of such information. Nevertheless, it is believed that the applied measures to protect the information systems of the armed forces can significantly reduce the risks of damage from the activities of external intruders. In conclusion, it is worth emphasizing

Information technology crime investigation systems require further modernization and improvement. The scientific community actively discusses emerging issues, which contributes to the formation of new regulatory initiatives. The main areas of development include:

1) more detailed legislative regulation of offences involving the use of digital means and stricter liability for such acts;

2) creation of a multi-level educational infrastructure for training specialists with deep knowledge in the field of modern computer science and information security;

3) adapting effective foreign cybercrime investigation practices while developing their own strategies to counter digital threats.

Further development of the field of cybercrime investigation involves the harmonization of domestic regulations with international standards in the field of cybersecurity. An integral part of these processes is the formation of specialized units in law enforcement agencies, as well as the introduction of a system of continuous professional training of employees in methods of collecting and analyzing digital evidence.

Of particular importance is the expansion of government cooperation with the private sector — it is technology companies that have unique knowledge and tools to effectively counter complex types of cyber attacks. Thus, the activity of solving crimes in this category is characterized by high dynamism and requires constant improvement of mechanisms for responding to new technological challenges. The effectiveness of the fight against cybercrime is determined by the speed of integration of applied expertise into existing legal procedures, strengthening international cooperation between relevant structures, and creating an adaptive legislative framework capable of responding in a timely manner to the rapidly changing digital threat landscape.

Literature:

1. Shevchenko, E. S. On the forensic interpretation of the concept of "cybercrime" // Information law. 2014. No. 3 (39).

2. Vekhov V. B. Computer crimes. Methods of commission, investigation methods. Moscow: Law and Law, 1996. Page 13.

3. Baturin Yu. M. Problems of computer law. Moscow: Legal lit., 1991. Page 72.

4. Krylov V. V. Information computer crimes. Moscow: INFRA-MNORMA, 1997. Page 25.

5. Kvyatkovsky K. S. Features of the personality of a criminal committing crimes in the field of computer information // Young scientist. 2022. No. 43 (438). P. 115–117.