Herald pedagogiki. Nauka i Praktyka

wydanie specjalne

Warszawa

Editorial Team

(wydanie specjalne) Volume-2, № 3 May 2022

ARCHIVING

*Sciendo archives the contents of this journal in **ejournals.id** - digital long-term preservation service of scholarly books, journals and collections.*

PLAGIARISM POLICY

*The editorial board is participating in a growing community of **Similarity Check System's** users in order to ensure that the content published is original and trustworthy. Similarity Check is a medium that allows for comprehensive manuscripts screening, aimed to eliminate plagiarism and provide a high standard and quality peer-review process.*

About the Journal

Herald pedagogiki. Nauka i Praktyka (HP) publishes outstanding educational research from a wide range of conceptual, theoretical, and empirical traditions. Diverse perspectives, critiques, and theories related to pedagogy – broadly conceptualized as intentional and political teaching and learning across many spaces, disciplines, and discourses – are welcome, from authors seeking a critical, international audience for their work. All manuscripts of sufficient complexity and rigor will be given full review. In particular, HP seeks to publish scholarship that is critical of oppressive systems and the ways in which traditional and/or "commonsensical" pedagogical practices function to reproduce oppressive conditions and outcomes.Scholarship focused on macro, micro and meso level educational phenomena are welcome. JoP encourages authors to analyse and create alternative spaces within which such phenomena impact on and influence pedagogical practice in many different ways, from classrooms to forms of public pedagogy, and the myriad spaces in between. Manuscripts should be written for a broad, diverse, international audience of either researchers and/or practitioners. Accepted manuscripts will be available free to the public through HPs open-access policies, as well as we planed to index our journal in Elsevier's Scopus indexing service, ERIC, and others.

HP publishes two issues per year, including Themed Issues. To propose a Special Themed Issue, please contact the Lead Editor Dr. Gontarenko N **(info@ejournals.id)**. All submissions deemed of sufficient quality by the Executive Editors are reviewed using a double-blind peer-review process. Scholars interested in serving as reviewers are encouraged to contact the Executive Editors with a list of areas in which they are qualified to review manuscripts.

TACTICS FOR THE PRODUCTION OF INVESTIGATIVE ACTIONS IN THE INVESTIGATION OF CYBERCRIME

Davronov Atobek Ravshanovich
PhD, Lecturer, Department of Criminal Procedure Law,
Tashkent state University of Law

Abstract: The article analyzes the investigation of crimes committed using IT technologies are considered. With the help of general scientific methods of cognition (analysis, synthesis, induction and deduction), the author came to the conclusion that high-quality initial investigative actions and operational-search measures, timely collection of evidence with the involvement of highly qualified specialists, appointment of special examinations affect the result, which will depend effectiveness in preventing and investigating computer crimes. The specificity of the investigation of crimes committed using the capabilities of IT technologies requires the development of new tactical approaches and techniques for the implementation of such an investigative action as interrogation and inspection of the scene, which will undoubtedly improve the efficiency of investigating crimes committed using the capabilities of IT technologies.

Keywords: Tactics, cybercrimes, information, investigations, Internet, supervision, cybersecurity, cybernetics, domain, investigations, investigator.

ТАКТИКА ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Давронов Атобек Равшанович
PhD, преподаватель кафедры Уголовно-процессуального право
Ташкентского юридического университета

Аннотация: В статье анализировано расследования преступлений, совершаемых с использованием IT-технологий. С помощью общенаучных методов познания (анализа, синтеза, индукции и дедукции) автор пришел к выводу, что качественно проведенные первоначальные следственные действия и оперативно-розыскные мероприятия, своевременный сбор доказательственной информации с привлечением высококвалифицированных специалистов, назначение специальных экспертиз влияют на результат, от которого будет зависеть эффективность предотвращение и расследование компьютерных преступлений. Специфика расследования преступлений, совершенных с использованием возможностей IT-технологий, требует разработки новых тактических подходов и приемов к осуществлению такого следственного действия, как допрос и осмотр место происшествия что, несомненно, позволит повысить эффективность расследования преступлений, совершенных с использованием возможностей IT-технологий.

Ключевые слова: Тактика, киберпреступления, инорфмация, расследования, Интернет, надзор, кибербезопастность, кибернетика, домен, следствия, следователь.

In the 21st century, in the era of the heyday of the information society, one of the major problems was the development of cybercrime. Along with the improvement of new technologies and the growing variety of social platforms within the global network, the number of users who are immersed in the virtual environment has also begun to increase. A natural process is the emergence along with a new sphere in human life and new types of crime associated with it. Cyberspace is no exception, because the Internet contains a large amount of personal data about people: data on documents, photos, location, passwords, personal correspondence and much more. Therefore, given the amount of information available on the Internet, we can conclude that not only individuals, but also entire states can be under threat.

According to Chapter VII. Strengthening the security and defense potential of the country, maintaining an open, pragmatic and active foreign policy of the Decree of the President of the Republic of Uzbekistan "On the development strategy of the new Uzbekistan for 2022-2026" dated January 28, 2022 №. UP-60, one of the main tasks was to create a cybercrime prevention system [1].

In addition, in accordance with the state plan for the implementation of the Development Strategy of New Uzbekistan for 2022-2026 in the Year of Human Dignity and Active Good Neighborhood, the tasks to combat cybercrime are:

1.Establish effective control over the investigation, further strengthen the operational-search activities in the fight against crimes committed with the help of information technology.

Mechanism for the implementation of this task: Supervision of investigative activities, reforming operational-search activities to identify new types of crimes committed using information technology, including cybercrime, mobilization of additional forces and means, as well as further improving the effectiveness of protecting the dignity and freedom of citizens in the fight with the specified crimes.

2.Complete the transformation of the banking system, bringing the share of private banks to 60% of all banking assets by 2025.

One of the mechanisms for the implementation of this task: ensuring cybersecurity in the provision of financial services.

3.Creation of a cybercrime prevention system.

The mechanism for implementing this task:

a)Development of the Cybersecurity Strategy of the Republic of Uzbekistan for 2023-2026.

At the same time, to determine the main directions of cybersecurity of the Internet space of the "UZ" domain zone, as well as complex tasks for the protection of e-government, energy, digital economy and other areas related to important information infrastructure.

b)Revisiting the criminalization of cybercrime.

c)Further improvement of the system for monitoring cyber attacks and threats in the information space.

Expansion of the technical infrastructure of the Unified Cybersecurity Network;

Further acceleration of the "IT Park of Innovations in Cybernetics";

The IT park will train young people in the basics of cybersecurity on the basis of digital technology training centers in the regions, as well as annually hold republican competitions to identify cyber-attacks among students and schoolchildren [2].

In the recommendations of the UN experts: "cybercrime" is any crime that can be committed with the help of a computer system or network, within a computer system or network, or against a computer system or network [3; P. 25].

In his study, T. M. Khusyainov gives the following interpretation: "The term "Internet crime" or "cybercrime" should be understood as the whole range of criminal actions in the field of information technology□"[4; P. 120].

M. E. Batukhtin describes a somewhat broader concept in his work: "cybercrime is any crime in the electronic sphere, committed with the help of computer means or a virtual network, or against them" [5; P. 28].

Cybercrime is a set of crimes committed in "cyberspace" with the help of or through computer systems or computer networks, as well as other means of access to cyberspace, within computer systems or networks, as well as against computer systems, computer networks and computer data. "Cybercrime" refers to any crime committed using various methods and means of creating, processing, transmitting computer information. [6; P. 12].

The term "cybercrime" is more extended than "computer crime", although sometimes they are used together or as synonyms, since "cybercrime" is a crime associated with both the use of computers and the use of information technology and global networks, and "computer crime" refers only to crimes committed against computers or computer data [7; P. 104-106].

According to the Law of the Republic of Uzbekistan "On Cybersecurity" dated April 15, 2022 No. ZRU-764, cybercrime is a set of crimes carried out in cyberspace using software and hardware in order to seize information, change it, destroy or hack information systems and resources [8; Art. 3].

When investigating cybercrime, there are a number of features that lie, firstly, in the detection, fixation and seizure of the trace left during the commission of a cybercrime, and secondly, in the lack of a clear understanding of what investigative actions should be carried out when investigating cybercrime and the correct sequence of the algorithm for conducting investigative actions. This happens because when investigating cybercrimes, investigators have to recognize and record not only material objects, but also the "cybernetic space" itself, formed by means of a computer network, an accessible segment of a local area network, the global Internet and digital media of computer information.

As a rule, the reason for initiating a criminal case are allegations of unauthorized access, embezzlement of funds. They come from organizations, much less often from citizens. The explanation for this may be that citizens are afraid of disclosure during the investigation of stolen information, which may contain secret, intimate and other details of their personal lives. Therefore, when such a situation arises, the investigator needs to establish psychological contact, explain to the citizen that the investigation is only interested in data that are relevant to the investigation of the crime and cannot be disclosed to third parties. [9; P. 131-132].

In the investigative tactics of cybercrime, it has always been of great importance to build a system of tactical methods for conducting investigative actions and tactical operations with the skillful and thoughtful use of various mental techniques. At present, when electronic media, information systems, social networks, accessed via the Internet, have become part of the daily life of citizens of the Republic of Uzbekistan, and with the introduction into their lives of the results of all modern scientific and technical research and the use of computer and Internet technologies have significantly expanded the social, labor, entrepreneurial horizons of the citizens of our country, which makes it possible to reasonably apply and use these achievements.

It should be noted that interrogation in criminal cases in the investigation of cybercrime has certain specifics. Of course, the investigation of cases in the field of computer information should be entrusted to an investigator who has a great knowledge of cybernetics. However, the analysis, as well as a survey of employees of law enforcement agencies related to the investigation of crimes in the field of high technologies, led to the conclusion that there is a catastrophic lack of such specialists in law enforcement. [10; P. 282-287].

The tactics of interrogation in criminal cases of this category directly depends on the specifics of the mechanism for committing a crime and other positive and negative factors. The first should include the presence of a certain amount of information about the criminal event obtained from various sources (during the preliminary verification of materials on the event under investigation, the results of operational-search measures), as well as about the person with whom the investigative action is to be carried out (obtained earlier in the course of his explanations, from protocols of procedural actions). Among the negative factors, one can include a significant period of time that has elapsed from the moment the crime was committed until the moment the interrogation was carried out. [11; P. 104-111].

It seems reasonable point of view of V. M. Bykov, who believes that the tactics of interrogation should be built taking into account the appropriate forensic type of interrogated. They identified the following types: active and inactive, conscientious victims, unstable, unscrupulous victims [12; P. 27-32].

The involvement of specialists in a number of investigative actions can help eliminate shortcomings in the knowledge and skills of the investigator. However, in some cases, the presence of a specialist in the version in which forensic scientists speak may be unjustified.

Basically, the tactics of investigative action, depending on the type of cybercrime, is divided into three stages:

The first stage is characterized by the following:

a)conducting athorough inspection of the scene, inspection of all computer equipment, communications, mobile devices, including the information environment;

b)seizure and inspection of documents, items, technical devices and electronic media;

c)detailed interrogation of the victim, suspect, witnesses;

d)detention of suspects and their personal search;

e)searches at the place of residence, work or possible rented premises of suspects;

f)appointment of various types of expertise, including computer, forensic, accounting, economic and other types.

The second and third investigative tactics are of a search and reconnaissance nature and are characterized by a similar list of investigative actions and operational search activities:

1)inspection of the scene of the incident, including inspection of computer equipment, tablets, mobile phones that belong to the victims or a certain organization;

2)interrogation of the victim (representative of the victim) and witnesses;

3)seizure and inspection of documents, objects, technical devices and electronic media;

4)sending requests for information of interest to the investigation to various organizations and companies (for example, telecom operators, credit organizations, etc.);

5)carrying out operational search activities in order to identify persons involved in the commission of a crime;

6)appointment of a special expert examination depending on the crime.

Let us pay attention to the fact that not all possible variants of typical investigative situations of the initial stage of the investigation are listed. Each investigative situation requires an individual approach to build the right algorithm for the actions of the investigator in order to give forensically significant information of probative value. At the same time, in some cases it is quite difficult to establish the signs of a crime within the time limit of the procedural verification of materials, which is associated with the specifics of the methods and means of committing a crime, and, consequently, the peculiarities of the mechanism of trace formation when working with computer information.

It is important to take into account that a number of technical devices, the operation of which is based on electromagnetic, x-ray radiation or a magnetic field, may affect the operation of nearby devices and the computer information stored on them. A person involved in the inspection as a specialist must be careful when working with technical means, as well as with powders and chemical reagents, especially if they need to process computer equipment.The specialist must be competent in the field of operation of technical means, the processes of functioning of computer systems and networks, and be fluent in technical terminology.

Despite the specifics of such inspections, the general inspection rules remain unchanged:

1)from general to particular;

2)from directories to individual files;

3)from the general characteristics of the file to its content.

Only those means of computer technology that contain or may contain forensically significant information should be seized.

According to R.A. Dryugen and M.A. Shergin, special modern hardware and software systems designed for these needs (for example, Mobile Forensicist, UFED, Belkasoft, SecureView 3, MOBILedit!, MicroSystemation, XRY, etc.) can contribute to better and faster removal of digital traces. As part of the inspection of the scene of the incident, their use allows you to extract the necessary information from technical devices that is important for the investigation of a criminal case. In law enforcement agencies, the most popular hardware and software systems "Mobile criminalist" and "UFED" [13; P. 100-104]. In our opinion, this is not an exhaustive list of software for detecting cybercrime.

In conclusion, it should be said that in a short period of time, forensic science has made significant progress in understanding how exactly it is necessary to investigate and disclose cybercrimes. Despite the fact that the formation of a clear list of investigative actions, the conduct of which will give the most significant results and information for the investigation, has not yet been completed, and the technical means used by law enforcement officers are still imperfect, it can be said with confidence that the detection of this type of crime, albeit at a slow pace, is growing. Further improvement of the tactics of conducting investigative actions, raising the level of skills of operational officers, investigators, experts and specialists, the development and implementation of the latest technical methods and means will ultimately lead to an increase in the quality of the investigation of such crimes.?

References:

1.Davronov A.R. Formation and development of the prosecutor's supervision over the compliance of laws in investigation of crimes in the sphere.- proacademy, 2021.

2.Davronov A.R. Prosecutor's supervision over the legality of the preliminary investigation and inquiry during the qualification of crimes in the - ProAcademy, 2021.

3.Davronov A.R. Analysis of terminological concept of information technologies in domestic and foreign literature. Review of law sciences, 2018.

4.Davronov A.R. Analysis of terminological concept of information technologies in domestic and foreign literature. № 1/7. 2019

5.Kudratillaev K. SPECIFIC FEATURES OF THE USE OF PRECAUTIONARY MEASURES //СОВРЕМЕННЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ. - 2022. - С. 215-218.

6.Кудратиллаев Х. З. ВОПРОСЫ ИМПЛЕМЕНТАЦИИ ПРОЦЕССУАЛЬНЫХ НОРМ МЕЖДУНАРОДНЫХ КОНВЕНЦИЙ ПО РЕГУЛИРОВАНИЮ АРЕСТА И КОНФИСКАЦИИ //Multidiscipline Proceedings of Digital Fashion Conference.- 2022. - Т. 2. - №. 2.

7.Абдуллоҳ Убайдуллоҳ Ўғли Нишонов МЕДИАЦИЯГА ТЕГИШЛИ ДОИРАДАГИ ИШЛАР ВА ҲУҚУҚИЙ ТАРТИБГА СОЛИШ МЕХАНИЗМЛАРИ // Scientific progress. 2021. №2. URL: https://cyberleninka.ru/article/n/mediatsiyaga-tegishli-doiradagi-ishlar-va-u-u-iy-tartibga-solish-mehanizmlari (дата обращения: 12.05.2022).

8.Mamatalieva S. K. INTERNATIONAL EXPERIENCE IN ENSURING THE PROTECTION AND SECURITY OF PARTICIPANTS IN CRIMINAL PROCEEDINGS BY THE STATE //Multidiscipline Proceedings of Digital Fashion Conference. - 2022. - Т. 2. - №. 2.

9.Mamatalieva S. K. ENSURING THE SAFETY OF WITNESSES IN CRIMINAL PROCEEDINGS //Multidiscipline Proceedings of Digital Fashion Conference.- 2022. - Т. 2. - №. 2.

10.Mamatalieva S. K. ENSURING THE SAFETY OF THE VICTIM AND WITNESS IN CRIMINAL PROCEEDINGS (On the example of the Russian Federation) // Herald pedagogiki. Nauka i Praktyka. - 2022. - Т. 2. - №. 2.

11.Mamatalieva S. K. SOME PROBLEMS OF THE PROSECUTOR'S PARTICIPATION IN CIVIL COURTS //Herald pedagogiki. Nauka i Praktyka. - 2022. - Т. 2. - №. 1.

12.Mamatalieva S. K. SOME PROBLEMS IN THE APPLICATION OF THE PROSECUTOR'S OPINION ON CIVIL PROCEDURE //Herald pedagogiki. Nauka i Praktyka. - 2021. - Т. 1. - №. 2.

13.Мавланов К. Жиноят ишлари юритувида гумон қилинувчига нисбатан қамоққа олиш тарзидаги эҳтиёт чорасини қўллаш //Общество и инновации. - 2021. - Т. 2. - №. 12/S. - С. 265-269.

14.Мавланов К. Т. ЖИНОЯТ ПРОЦЕССИДА ГУМОН ҚИЛИНУВЧИНИНГ ИШ МАТЕРИАЛЛАРИ БИЛАН ТАНИШИШ ҲУҚУҚИНИ ТАЪМИНЛАШ //

ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ. - 2021. - Т. 6. - №. 2.

15.Мавланов К. Т. ЖИНОЯТ ПРОЦЕССИДА ГУМОН ҚИЛИНУВЧИ ҲУҚУҚЛАРИНИ КАФОЛАТЛАШГА ҚАРАТИЛГАН ХАЛҚАРО СТАНДАРТЛАР //ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ. - 2020. - Т. 5. - №. 12.

16.Мавланов К. Жиноят процессида айбсизлик презумпцияси: миллий ва хорижий тажриба //Общество и инновации. - 2021. - Т. 2. - №. 2/S. - С. 16-22.

17.Мавланов К. Айрим ривожланган хорижий мамлакатлар қонунчилигида жиноят содир этишда гумон қилинаётган шахснинг ҳимоя ҳуқуқи билан таъминланганлик ҳолати //Общество и инновации. - 2021. - Т. 2. - №. 1/S. - С. 96-103.

18. Decree of the President of the Republic of Uzbekistan "On the development strategy of the new Uzbekistan for 2022-2026" dated January 28, 2022 No. UP-60.

19.Development strategies of New Uzbekistan for 2022-2026 in the "Year of human dignity and active good neighborliness" 2 appendix.

20.Report of the X UN Congress on the Prevention of Crime and the Treatment of Offenders // Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders. 2000. Chapter 5. C. 25 file:///C:/Users/Admin/Downloads/ A_CONF.187_15-EN.pdf. Date of access: 31.05.2022.

21.Khusyainov T. M. Internet crimes (cybercrimes) in the Russian criminal law // Criminal law of the Russian Federation: Problems of law enforcement and prospects for improvement Materials of the All-Russian round table. 2015. P. 120

22.Batukhtin M. E. Cybercrimes: causes, types, forms, consequences, directions of counteraction // Problems and prospects for the development of the penitentiary system of Russia at the present stage Proceedings of the International scientific conference of adjuncts, graduate students, cadets and students. 2018. S. 28.

23.Glotina I.M. Cybercrime: Main manifestations and economic consequences // Issues of Economics and Law. - 2014. - No. 8. S. 12.

24.Serieva M. M. Cybercrime as a new criminal threat // New Legal Bulletin. - 2017. - No. 1. pp. 104-106.

25.Law of the Republic of Uzbekistan "On Cybersecurity" dated April 15, 2022 No. ZRU-764. Art. 3.

26.Kharina E.N. On the possibilities of using the Internet in the investigation of crimes / E.N. Kharina // Current state and prospects for the development of scientific thought: materials of the Intern. scientific-practical. Conf., Ufa, May 25, 2015: at 2 o'clock - Ufa: Aeterna, 2015. - Part 2. - S. 131-132.

27.Kolominov V.V. Tactics for the production of individual investigative actions in the investigation of cybercrimes. Collection of scientific articles based on the materials of the All-Russian Scientific and Practical Conference (with international participation), dedicated to the 20th anniversary of the Department of Criminalistics. Modern problems of domestic criminalistics and prospects for its development. pp. 282-287.

28.Smirnova I. G., Kolominov V. V. Tactical features of interrogation in cases of crimes in the sphere of computer information. Izvestiya of the Irkutsk State Economic Academy. Electronic scientific journal. 2015. V. 6. No. 3. S. 104-111.

29.Bykov V. M. Interrogation of the victim / V. M. Bykov // Legality. 2014. No. 6. S. 27-32.

30.Dryugena R.A., Shergina M.A. On some features of the investigation of crimes committed with the use of it-technologies and in the field of computer information. Zh: Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia No. 3 (31) 2021. P. 100-104.

31.Rakhimova, U. (2020) "Cybercrime subject and limits of proof", TSUL Legal Report International electronic scientific journal, 1(1). -P.103.Available at: https://legalreport.tsul.uz/index.php/journal/article/view/17.

32.Рахимова, У. (2021). История становления судебной экспертизы в
республике Узбекистан. Общество и инновации, 2(1/S), 270-274.

33.Рахимова, У. Х. (2019). Понятие, значение и особенности производства по делам о примирении. Молодой ученый, (47), 364-366.