Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Digital traces in forensic science: concepts, classifications, and challenges

Bakhtiyor Khamidov [1]

Tashkent State University of Law

ARTICLE INFO

Article history:
Received July 2025
Received in revised form
15 July 2025
Accepted 25 July 2025
Available online
15 August 2025

Keywords:
digital traces,
electronic traces,
information traces,
binary traces,
virtual traces,
forensic science,
cybercrime.

ABSTRACT

This article examines the scientific and theoretical foundations of the concept of digital traces. Particular attention is given to a critical analysis of various definitions and classifications proposed by scholars in the United States, Russia, Europe, and the CIS countries. The study argues that the concept of a digital trace should primarily be defined according to its technical characteristics. In this context, the paper compares and evaluates such notions as electronic traces, information traces, binary traces, virtual traces, and digital traces.

The author emphasizes that with the rapid development of digital technologies, traces may arise not only as a result of human activity but also as a consequence of technical or cyber processes. Special attention is devoted to the distinction between active and passive types of digital traces, as well as to their content, form, and technical properties.

The article is based on a combination of theoretical and practical research, drawing upon both scholarly discussions and empirical findings. The conclusions are intended to contribute to the advancement of forensic science by clarifying the essence of digital traces and their role in the administration of justice.

2181-1415/© 2025 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol6-iss7/S-pp462-478

Sud ekspertizasidagi raqamli izlar: tushunchalar, tasniflar va muammolar

Kalit so'zlar:
raqamli izlar,
elektron izlar,

ANNOTATSIYA

Ushbu maqola raqamli izlar kontseptsiyasining ilmiy va nazariy asoslarini o'rganadi. AQSh, Rossiya, Yevropa va MDH

[1] Tashkent State University of Law. Senior teacher of the department of Criminalistics and Forensics Investigation
E-mail: Bahtiyor1984bsj@mail.ru

axborot izlari,
ikkilik izlar,
virtual izlar,
sud ekspertizasi,
kiberjinoyat.

mamlakatlari olimlari tomonidan taklif etilgan turli ta’riflar va tasniflarni tanqidiy tahlil qilishga alohida e’tibor beriladi. Tadqiqot shuni ko'rsatadiki, raqamli iz tushunchasi birinchi navbatda uning texnik xususiyatlariga ko'ra belgilanishi kerak. Shu nuqtai nazardan, maqola elektron izlar, axborot izlari, ikkilik izlar, virtual izlar va raqamli izlar kabi tushunchalarni taqqoslaydi va baholaydi.

Muallifning ta'kidlashicha, raqamli texnologiyalarning jadal rivojlanishi bilan izlar nafaqat inson faoliyati, balki texnik yoki kiber jarayonlar natijasida ham paydo bo'lishi mumkin. Raqamli izlarning faol va passiv turlarini farqlashga, shuningdek, ularning mazmuni, shakli va texnik xususiyatlariga alohida e'tibor beriladi.

Maqola ilmiy munozaralar va empirik xulosalarga asoslangan nazariy va amaliy tadqiqotlar kombinatsiyasiga asoslangan. Xulosalar raqamli izlarning mohiyatini va ularning odil sudlovni amalga oshirishdagi rolini oydinlashtirish orqali sud-tibbiyot fanining rivojlanishiga hissa qo'shishga qaratilgan.

Цифровые следы в криминалистике: концепции, классификации и проблемы

Ключевые слова:
цифровые следы,
электронные следы,
информационные следы,
бинарные следы,
виртуальные следы,
криминалистика,
киберпреступность.

АННОТАЦИЯ

В данной статье рассматриваются научно-теоретические основы понятия «цифровой след». Особое внимание уделяется критическому анализу различных определений и классификаций, предложенных учёными США, России, Европы и стран СНГ. В статье утверждается, что понятие «цифровой след» следует определять, прежде всего, с учётом его технических характеристик. В этом контексте сравниваются и анализируются такие понятия, как «электронный след», «информационный след», «бинарный след», «виртуальный след» и «цифровой след».

Автор подчёркивает, что в условиях стремительного развития цифровых технологий следы могут возникать не только в результате человеческой деятельности, но и в результате технических или киберпроцессов. Особое внимание уделяется различию активных и пассивных типов цифровых следов, а также их содержанию, форме и техническим свойствам.

Статья основана на сочетании теоретических и практических исследований, опираясь как на научные дискуссии, так и на эмпирические данные. Выводы статьи призваны способствовать развитию криминалистической науки, проясняя сущность цифровых следов и их роль в отправлении правосудия.

INTRODUCTION

In traditional forensic science, research has largely focused on two main categories of traces: material and ideal [1, p. 66]. However, the conceptual foundations of digital traces remain insufficiently explored in the scientific literature of Uzbekistan. This lack of theoretical development creates practical challenges for law enforcement agencies when identifying sources of digital evidence and complicates the process of building a comprehensive forensic methodology in this field. Consequently, there is a pressing need for forensic research that addresses the specific characteristics of digital traces and establishes evidence-based approaches for their use in criminal investigations.

With the rapid growth of digital technologies, digital traces have significantly increased in volume compared to physical traces. In modern society, digital technologies permeate nearly all spheres of life and have become essential for performing daily tasks, shaping individual lifestyles, and influencing social interactions. Human activity now occurs simultaneously in both the material world and the digital environment. Naturally, this dual activity leaves behind digital footprints that can later serve as sources of evidence in criminal proceedings [2, p. 263]. Thus, investigators must possess a clear understanding of the concept, content, forms, and specific features of digital traces in order to effectively investigate cybercrime.

Forensic examination of crime traces has always possessed unique features. Unlike conventional crimes, cybercrimes are often committed remotely. Offenders use digital means to exert influence on the target of their crime while simultaneously concealing the traces of their actions. This creates specific challenges for law enforcement, as digital traces are not only highly dynamic but may also be deliberately altered or erased in order to resist investigation. Therefore, understanding the nature and technical properties of digital traces is essential for ensuring the accuracy and admissibility of digital evidence in criminal justice.

MATERIALS AND METHODS

This study analyzes the theoretical approaches to the concept of digital traces developed by criminologists and forensic scientists in the United States, Russia, Europe, and the CIS countries. The aim is to evaluate the applicability of these concepts in the context of Uzbekistan and to identify the most consistent and technically accurate definition of a digital trace.

The research relies on a critical review of the literature, with special attention to debates surrounding the use of terms such as *electronic traces*, *information traces*, *binary traces*, *virtual traces*, and *digital traces*. Through this analysis, the author seeks to determine which concept most accurately reflects the technical and forensic essence of digital evidence.

Methodologically, the study employs both general and specific scientific approaches. General methods include **analysis, synthesis, induction, and deduction**, which are used to examine and systematize theoretical views. In addition, a **comparative legal method** is applied to evaluate foreign forensic concepts and their relevance to Uzbekistan. Finally, elements of **technical-legal analysis** are employed to explore the technological characteristics of digital traces and their implications for forensic practice.

RESEARCH RESULTS

General Theoretical Perspectives on Digital Traces

In the forensic literature, scholars have proposed various terms to describe traces left in digital environments. These include *electronic traces* [3, p. 77], *information traces* [4, p. 55], *binary traces* [5, p. 163], *virtual traces* [6, p. 15; 7, p. 152; 8, p. 45; 9, p. 125; 10, p. 87; 11, p. 30; 12, p. 129], and *digital traces* [13, p. 117; 14, p. 23; 15, p. 61]. To determine which of these definitions most accurately reflects the nature of forensic evidence, it is necessary to examine their essence and technical characteristics in detail.

Electronic traces

In V. Vekhov's studies, the concept of an electronic trace is put forward. The scientist considers electronic traces as electronic information carriers and information of forensic significance stored in their memory. According to him, electronic traces are also stored in objects that receive and reflect the trace. An object that receives a trace not only reflects the trace, but is also its carrier. In this case, information passes from one system to another in the form of a signal on certain material carriers.

A signal is the most physical medium, especially electromagnetic signals. It includes information content and form. A specific property of an object or reflection of an event constitutes the content of the signal. Reflecting, storing or transmitting means that make up its material basis are signal forms [16, 78 p.].

In fact, all kinds of digital devices now run on electricity. It is the ordered movement of charged particles that serves as the main resource - a tool in the creation, processing, storage, transmission or performance of some other functions of digital information. However, the processor "remembers" the numbers, not the signal, that is, it encodes it.

At the same time, a specific form of electric current (signal, electromagnetic signal, magnetic field) does not exist in nature. V. B. Vekhov did not show the technical aspects of this in his study. Therefore, we can assume that the concept of an electron does not have sufficient scientific justification.

Logically, how can you see, read or remove traces from an object that has no form?!

Solving these issues is fundamentally important when investigating cybercrime! The reason is that the inquirer, investigator, prosecutor, judge, lawyer assess the circumstances that are important for the case from a legal point of view, and administer justice. Lack of understanding of the nature of digital evidence and its specific characteristics makes it difficult to verify and assess the true state of affairs.

In the course of scientific and technical research, it was found that the concept of "electronic" is a logically incorrect concept. At the same time, it was concluded that the electric current is involved only as a tool in the processes associated with the creation, processing, storage, transmission and transportation of digital information [17, 265 p.]. Accordingly, the author puts forward the idea that any information on a digital device is only in a single form, that is, in digital form.

Information traces

The concept of "information traces" is also not accepted by most legal scholars. This is because the concept does not really capture the technical nature of digital footprints, but is simply used as a metaphor in theory. Accordingly, it can be considered that this concept is also used inappropriately.

Binary traces

The concept of "binary traces" is not erroneous, but technically in modern digital devices the processor works with combinations of "0" and "1" binary or "0", "1", "2" ternary codes. From a practical point of view, the concept of "binary traces" is typical for most digital devices, but this category is not the only one in theory.

Virtual traces

An analysis of scientific research shows that the concept of "virtual traces" is the subject of heated discussions in theory. Before proceeding to the discussion, let us briefly dwell on the meaning of the term “virtual”.

Sources indicate that the origin of the term "virtual" dates back to the 15th century. In English literature, the term "virtual" comes from the Latin words "virtus", "virtualis", which means "having an effect, not having any form or appearance" [18]. However, since 1959, this term has been used in the field of digital technologies in the sense of “something that does not exist materially, but created with the help of a program” [19].

According to Vekhov V.V., the concept of “virtual” comes from the Latin word “virtualis”, which means something that has no material scope or is perceived differently than it is actually realized [20, 84 c].

A.B. Smushkin believes that virtual traces are traces left by any movement made in the information environment of computers and other digital devices, their systems and networks [21, 44 c].

According to V.A. Meshcheryakov, the concept of "virtual traces" as any change in an automated information system associated with a crime event, recorded in the form of computer information [22, 101 p.]. Each of the above definitions is related to digital resources.

In the Russian-Uzbek explanatory dictionary of terms related to operating systems and computer networks, the word "virtual" is defined as "an object or state that does not really exist, but may appear under certain conditions" [23, 98 p.]. It is noteworthy that in all three cases, such aspects of the concept as “having no material appearance” or “non-existent in practice” form a commonality. Therefore, the word virtual can be understood as a reality or a property that does not have materiality, but really exists.

Currently, this concept is used in the field of information technology as a place - an environment where digital information is created, stored, processed or other actions related to it are performed. Therefore, the concept of virtual footprints does not essentially reflect the shape and characteristics of digital footprints. In our opinion, this concept is inappropriate in relation to this situation, since the theoretical basis is not sufficiently substantiated.

Digital traces

There are different opinions in the scientific community about digital footprints. For example, S.A. Zaitsev and V.A. Smirnov define digital traces as a set of certain actions performed by a user in the global network or associated with other digital media [24, 81 p.]. This definition does not cover traces left on a digital device or as a result of a cyber process. Therefore, it can be considered that there are certain shortcomings in the definition.

N.I. Malykhina described these traces as changes in the memory of telecommunication systems as a result of a crime [25, 205 s]. Although the definition is relatively correct, the author has defined its limits in a narrow circle. The reason is that

the concept of digital footprints extends not only to criminal proceedings, but also to other branches of law.

J. Moteshko and M. Moteshkova prefer the following definition: a digital footprint can be defined as any information that is stored or transmitted in digital form and that is associated with the event under investigation, with which it can be found, early and detailed investigation and decoding using modern forensic or forensic methods and means [26, 218 p.]. This description can be considered relatively complete. However, this definition also has the following disadvantages:

First, the transfer of digital footprints is a relatively contentious issue. Therefore, in the processes of investigation and examination, in the prescribed manner, it is not the transferred traces that are studied and evaluated, but the preserved traces. If the cyber process (criminal activity) relevant to the case is at the stage of preliminary investigation or trial, such a situation is subject to investigation in accordance with the established procedure. Otherwise, it is impossible to ensure the admissibility of evidence;

secondly, the concepts of "digital footprint" and "digital evidence" differ from each other in theory and in practice. For example, the concept of "digital footprint" is a forensic concept, as the authors point out, and "digital evidence" is a category within the criminal procedure law. In other words, the category of digital evidence is determined in different jurisdictions within a certain procedural order. Therefore, it is appropriate to clarify this in the definition.

ANALYSIS OF THE RESEARCH RESULTS

In our opinion, digital footprints should be understood as the result of any activity that occurs in the digital environment. Because digital traces are created not only by the user, but also as a result of certain technical or cyber processes.

It should be noted that digital footprints are caused not only by the human factor, but can also occur as a result of a certain cyber process. The reason is that now malware has the ability to change its code and leave various traces.

When establishing the truth in a case, it is necessary to collect, verify and evaluate the traces left in digital sources. These digital resources include:

information processing systems or individual functional units of such systems;

personal computers, laptops, netbooks, system blocks and networks;

digital media (hard and soft magnetic disks, flash drives, memory cards, optical disks, etc.);

navigators, trackers;

may include mobile communication devices and SIM cards, digital radios, plastic payment cards and skimmers, slot machine cards, VCRs and other similar sources.

Digital information is the basis of digital footprints. Digital information functions with the help of certain programs. Therefore, its functionality is built on the basis of the software architecture.

Engineers have divided the system into "Frontend" and "Backend" parts so that the software works correctly. The "Frontend" part is the presentation part of the software and is the user interface. Typically, this section covers the components that are visible to the user when the digital device is turned on.

The "Backend" part is the backbone of the software system. At the same time, the codes are written in such a way that the functions in the presentation part of the software work correctly. Typically, these codes consist of a specific letter, number, and symbol.

These codes are converted into combinations of "0" and "1" by the assembler or compiler for reading by the processor.

Both parts store the history of user actions. However, it is not always possible to obtain data from Frontend in forensic investigations. Therefore, experts use special programs to study traces in the Backend.

Types of digital footprints

In foreign sources, active and passive types of digital traces are distinguished [27, 39 p.].

Active footprints are footprints voluntarily left on a system or network of digital devices. For example, a user leaves comments on social networks or websites, publishes articles or data left in a keylogger. The keylogger records any changes made by the user to the clipboard. For example, a keylogger stores information that a user copies passwords or takes screenshots of confidential information.

The process of collecting and checking active traces has a relatively simpler appearance than passive traces. These can be social media profiles, emails and messages, blog posts and comments, file downloads, purchases, photos and videos, web searches, etc.

Social media

Social networks are the main source of active digital footprints. These networks include certain files (text, photo, audio, video, multimedia, etc.). Activities such as uploading or downloading, leaving a message, visiting other websites using a person's financial information, connecting with friends and contacts, joining dating sites or their applications generate certain digital footprints from themselves.

Email

When corresponding by e-mail, information about the person, contacts and sent or received letters is analyzed. When e-mail messages are transmitted or saved, certain log files remember and record the commands given by the user. Subsequently, digital footprints and evidence relevant to the case are extracted from these logs.

Block posts and comments

Blogs, forums, and other online communities can also be the source of such footprints. Usually such traces are left when a user posts a blog entry on certain sites or comments on them.

Downloads

In the process of downloading digital information, information about digital materials is generated. During the download process, the cache creates information confirming that the file has been downloaded. So, depending on this information, you can determine from which source the downloaded file was (text, photo, audio, video, etc.). This also applies to copyrighted material.

Photo and video

Photos and videos that are posted on the Internet also leave certain traces. In this case, information about who uploaded the photo or video, when it was uploaded, and where it was taken is stored in the file's metadata [30, 19; 31, 190 pp.].

It should be noted that information uploaded on social networks or websites such as YouTube is constantly monitored and stored. This information can provide basic information about a person's online activities, interests, or values.

Web search engines

What the user searches on the Internet, search terms are recorded and tracked by search engines. For example, the Google search engine analyzes information about the user and provides information about their interests or queries. Therefore, it would be useful for law enforcement agencies to analyze the Internet traffic of a suspect, accused, defendant or victim in order to establish the truth. This method is one of the most effective tools for studying the personality of a criminal.

Online shopping

Online stores are another source of active digital footprints. These may include:

making payments through commercial websites;

creating a subscription or accounts for coupons (discounts);

downloading and using the application for purchase;

subscription to brand newsletters, etc.

When shopping online, it tracks where, when and for what amount the product was purchased, as well as credit / debit card information.

Online banking

A set of services that allows you to perform various banking operations remotely via the Internet. The analysis shows that this type of online service is growing rapidly in the country. Typically, users download the application of a particular payment institution on their computer or mobile phone. Through the online banking service, the user can make payments, control transaction processes or receive reports at any time at his workplace or in other convenient conditions. These traces are left when you use the applications of various payment institutions, buy or sell stocks, subscribe to financial publications and blogs, open a credit card account or transfer funds to accounts.

Passive traces are traces that are automatically left on web resources when a user accesses the network. For example, cookies, user IP address, search history, etc.

Cookies

The piece of data that remains when you connect to a web server. This information determines:

the time of visiting the web page and the type of digital device;

the perpetrator's interests (such as language, currency, or hobbies);

perpetrator's requests;

IP address and location information;

operating system and browser version;

clicks and transitions.

IP address

A unique digital identifier that allows a digital device to connect to the Internet. The IP address determines the area where the offender is connected to the network. Theoretically, there are several types of IP addresses. However, identifying static or dynamic IP addresses is important in criminal investigations. Because, the offender's MAC address is determined by the IP address.

Location Information

This information is important in determining the whereabouts of the perpetrator. In most cases, digital devices that support GPS (smartphone, tablet) collect location data when connected to the Internet. Location data can be tracked even when the digital device is inactive.

Stalking traces

Surveillance cameras, facial recognition software, and other technologies also allow unauthorized surveillance, collection, distribution, stalking, and other malicious use of personal information.

For example, in mid-June 2021, it became known that South Korea's advanced technology had caused a whole wave of digital crimes in the field of sexual blackmail. About 14% of women living in Seoul suffered from digital sexual violence, including spy cam footage, unwanted intimate pictures, and distribution of videos of sexual acts, according to a survey from the EHV [29].

Other traces

Telecommunication service providers also store information about the activities of customers on the Internet. With these traces, visits, calls, messages, location data, IP addresses, and all activities related to online activities can be collected, monitored and evaluated.

Technical features of digital traces

Digital traces, like other traces in forensic science, have common and individual specifics. Digital footprints are left as a result of the action of a person - a user, a criminal, application or system software, the functionality of a digital device, or the automatic interaction of one device with another, a cyber process. Digital footprints have the following features:

digital footprints only occur in a digital environment;
have the ability to change
occur at the right time;
have a large volume;
have a variety of formats;
have the ability to detect and recover.

CONCLUSIONS

An analysis of the studies allows us to conclude that the concept of a digital footprint should be defined on the basis of specifics. The concept is based on the technical features of digital footprints. These traces originate in the digital environment and are considered the main means of establishing the truth in the administration of justice.

For the collection, storage, transportation and study of digital traces in the course of the investigation [32, 294; 33, 242; 34, 73, 35, 27 pp.] require special tools for digital forensics. At the same time, it is advisable that the law enforcement officer (investigator, investigator, prosecutor and court) have special training in working with digital traces and their evaluation.

REFERENCES:

1. Kriminalistika. Uchebnik. Kollektiv avtorov. [Criminalistics] T.: TGYU, 2019, 66 p.
2. Astanov , I. i Xamidov , B. 2021. Obtsheteoreticheskie voprosi, svyazannie s elektronnimi ili tsifrovimi dokazatelstvami: problema i reshenie. Obtshestvo i innovasii. [General theoretical issues related to electronic or digital evidence: problem and solution] 2, 7/S (avg. 2021), 259–278. DOI:https://doi.org/10.47689/2181-1415-vol2-iss7/S-pp259-278.
3. Vexov V.B. "Elektronnaya kriminalistika":chto za etim ponyatiem? [Electronic criminalistics":what is behind this concept?] / V.B. Vexov // Problemi

sovremennoy kriminalistiki i osnovnie napravleniya ee razvitiya v XXI veke: materiali Mejdunar. Nauch-prakt. konf. [Problems of modern criminalistics and the main directions of its development in the XXI century: materials of the International Scientific and Practical Conference] / pod Red. A.A. Belyakov, D.V. Baxteev, V.V. Biryukov, – Ekaterinburg: Izdatelskiy dom Urgyuu, 2017, pp 77-83.

4. Shapovalova G.M. Vozmojnost ispolzovaniya informatsionnix sledov v kriminalistike (voprosi teorii i praktiki): Diss. kand. kand. yurid. nauk. – Vladivostok, 2005. – 210 s.

5. Milashev V.A. Problemi taktiki poiska, fiksatsii i iz'yatiya sledov pri nepravomernom dostupe k kompyuternoy informatsii v setyax EVM: avtoref. dis. kand. yur. nauk. M., 2004. – 208 s.

6. Kirsanova S.O., Kalinina A.A. Virtualnie sledi: ponyatiye, sushnost, problemi / S.O. Kirsanova, A.A. Kalinina // Voprosi studencheskoy nauki. – 2018. № 3 (19). – S. 14-17. URL: https://cyberleninka.ru/article/n/virtualnye-sledy-ponyatie-suschnost-problemy (data obrasheniya: 07.11.2019).

7. Agibalov V.Yu. Virtualnie sledi v kriminalistike i ugolovnom protsesse.-M.: Yurlitinform, 2012.-152 s.

8. Smushkin A.B. Virtualnie sledi v kriminalistike / A.B. Smushkin // Zakonnost.-2012.-№ 8. - S. 43-48.

9. Shorin I.Yu., Shatilo Ya.S. Osobennosti sledov kompyuternix prestupleniy / I.Yu. Shorin, Ya.S. Shatilo // Informatika v sudebnoy ekspertize: sb. trudov. Saratov: SYUI MVD Rossii, 2003.-S. 124-127.

10. Kuzmin I.A. O formirovanii federalnogo ekspertno-kriminalisticheskogo ucheta virtualnix sledov prestupleniy / I.A. Kuzmin // Yevraziyskaya advokatura.-2019.-№1 (38).-S. 86-88 URL: https://cyberleninka.ru/article/n/o-formirovanii-federalnogo-ekspertno-kriminalisticheskogo-ucheta-virtualnyh-sledov-prestupleniy (data obrasheniya: 01.12.2019).

11. Mesheryakov V.A. «Virtualnie sledi» pod «Skalpelem Okkama» / V.A. Mesheryakov // Informatsionnaya bezopasnost regionov.-2009.-№1. – S. 28-33. URL: https://cyberleninka.ru/article/n/virtualnye-sledy-pod-skalpelem-okkama (data obrasheniya: 01.12.2019).

12. Cherkasov V.N., Nexoroshev A.B. "Virtualnie sledi" v "kiberneticheskom prostranstve" / V.N. Cherkasov, A.B. Nexoroshev // Sudebnaya ekspertiza: mejvuz. SB. Nauch. st.-VIP. 2.-Saratov: Syui MVD Rossii ["Virtual traces" in the "cybernetic space" / V.N. Cherkasov, A.B. Nekhoroshev // Forensic examination: mezhvuz. sb. scientific. art.-Issue 2.-Saratov: SIU of the Ministry of Internal Affairs of Russia]. 2003, pp. 127-130.

13. Semikalenova Anastasiya Igorevna (2019). Sifrovie sledi: naznacheniye i proizvodstvo ekspertiz. Vestnik Universiteta imeni O. Ye. Kutafina, (5 (57)), 115-120.

14. Davidov Vladimir Olegovich, & Tishutina Inna Valeriyevna (2020). Sifrovie sledi v rassledovanii distansionnogo moshennichestva. Izvestiya Tulskogo gosudarstvennogo universiteta. Ekonomicheskiye i yuridicheskiye nauki, (3), 20-27. doi: 10.24411/2071-6184-2020-10303

15. Khamidov B. KH, Kariov B.Z, Topildiyeva D.M General Theoretical Issues of Improving Private Forensic Methods In The Field Of Combat Against Cybercrime. PSYCHOLOGY AND EDUCATION (2021) 58(1): 2705-2712. ISSN:00333077/ 2021.

16. V.B. Vexov. «Elektronnaya kriminalistika»: chto za etim ponyatiyem? Problemi sovremennoy kriminalistiki i osnovnie napravleniya yee razvitiya v XXI veke: Materiali Mejdunarodnoy nauchno-prakticheskoy konferensii, posvyashennoy 60-letnemu yubileyu kafedri kriminalistiki Uralskogo gosudarstvennogo yuridicheskogo universiteta (6 oktabrya 2017 goda). – Yekaterinburg: Izdatelskiy dom Uralskogo gosudarstvennogo yuridicheskogo universiteta, 2017. – 81 s. [77-83]

17. Astanov , I. i Xamidov , B. 2021. Obsheteoreticheskiye voprosi, svyazannie s elektronnimi ili sifrovimi dokazatelstvami: problema i resheniye. Obshestvo i innovatsii. 2, 7/S (avg. 2021), 259–278. DOI:https://doi.org/10.47689/2181-1415-vol2-iss7/S-pp259-278.

18. https://www.merriam-webster.com/dictionary/virtual

19. https://www.etymonline.com/word/virtual

20. 20. Vexov V.B. Osnovi kriminalisticheskogo ucheniya ob issledovanii i ispolzovanii kompyuternoy informatsii i sredstv yee obrabotki: monografiya. Volgograd: VA MVD Rossii, 2008. S. 84

21. Smushkin A.B. Virtualnie sledi v kriminalistike // Zakonnost. 2012. Vip. 8. S. 43-45.

22. Mesheryakov V.A. Prestupleniya v sfere kompyuternoy informatsii: osnovi teorii i praktiki rassledovaniya // Izdatelstvo Voronejskogo gosudarstvennogo universiteta. 2002. S. 94 – 119

23. Djalalov M. Kovaleva R.: Operatsion tizimlar va kompyuter tarmoqlariga oid atamalarning ruscha-o‘zbekcha izohli lug‘ati. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. T.: 2018. 98-bet.

24. Zayseva S.A., & Smirnov V.A. (2021). AKSIOLOGICHESKIY PODXOD K PONYATIYU SIFROVOGO SLEDA. Noosfernie issledovaniya, (3), 79-87.

25. Malixina N.I. Kriminalisticheskoye izucheniye litsa, sovershivshego prestupleniye: teoretiko-prikladnie problemi / pod red. A.F. Volinskogo / N.I. Malixina. – Moskva : Yurlitinform, 2016. – 312 s.

26. .Metenko, M.Metenkova. Digital trace and their attributes evaluate for criminalistics. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. № 2 218 с.

27. Giardin, Fabien; Calabrese, Francesco Fiore, Filippo Dal; Ratti, Carlo; Blat, Josep. Digital Footprinting: Uncovering Tourists with User-Generated Content (англ.) // IEEE Pervasive Computing : journal. – 2008. – Vol. 7, no. 4. – P. 36– 43. – doi:10.1109/MPRV.2008.71.

28. https://cbu.uz/uz/payment-systems/remote-banking-services/

29. South of Korea becomes a global centre for digital sex crimes

30. Утепов, Д. и Каримов , Б. 2022. Проблемные вопросы противодействия торговли людьми в социальных сетях в Республике Казахстан. Общество и инновации. 3, 9/S (окт. 2022), 16–23. DOI:https://doi.org/10.47689/2181-1415-vol3-iss9/S-pp16-23.

31. Абулхайров, Р. (2022). Портлашдан кейин ҳодиса жойини кўздан кечиришда дастлабки тайёргарлик босқичининг криминалистик жиҳатлари: кўздан кечиришда иштирок этувчи тезкор гуруҳнинг таркиби ва уларнинг вазифалари. Eurasian Journal of Law, Finance and Applied Sciences, 2(12), 188-194.

32. Топилдиева, Д. 2022. Проблемы расследования киберпреступлений. Общество и инновации. 2, 11/S (янв. 2022), 292–296. DOI:https://doi.org/10.47689/2181-1415-vol2-iss11/S-pp292-296.

33. Абдуллаев Рустам (2020). Правовые вопросы сбора и использования цифровых доказательств в уголовном судопроизводстве. Review of law sciences, 3 (Спецвыпуск), 240-244. doi: 10.24412/2181-919X-2020-3-240-244.

34. Azim Baratov. (2022). INVESTIGATORY VERSIONS AND PLANNING FOR INVESTIGATION OF CRIMES RELATED TO ROBBERY AND PILLAGE COMMITTED IN A HOUSING. The American Journal of Social Science and Education Innovations, 4(11), 68–76. https://doi.org/10.37547/tajssei/Volume04Issue11-13

35. Akhmedova, G. (2022). ISSUES OF LEGAL REGULATION OF SEARCH ACTIVITY: FOREIGN EXPERIENCE. The American Journal of Political Science Law and Criminology, 4(11), 24-29.