Western European Journal of Linguistics and Education
Volume 2, Issue 7, July, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed

THE ROLE AND SIGNIFICANCE OF VIRTUAL ASSETS IN CYBERCRIMES

Goyibkulov Obidjon Orolovich
Investigator for particularly important cases of the Investigation Department under the Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract: The legal and forensic aspects of the collection and use of virtual traces in the investigation of crimes committed using information technologies are considered. Modern investigative practice in identifying and investigating cybercrimes is analyzed. The problems arising in the investigation of cybercrimes are explored.
Key words: cybercrime, virtual traces, digital evidence.

Introduction. In the era of digital technologies, the development of the information and communication technology system, which has penetrated into all areas of our life, requires participation in international and regional relations related to this area, as well as protection of this area from modern cyber threats. The rapid development of information and communication technologies has led to the introduction of information services provided by various computer technologies in wide areas of society.

This, in turn, prompted the emergence of a new field of cyber law. In general, the emergence of the field of cyber law was caused by:

- the emergence of virtual legal relations;
- ICT development;
- the need to ensure information security;
- current need for digital economy;
- The need to protect intellectual property rights on the Internet.

We live in the era of information society, where computers and telecommunication systems cover all spheres of human and state life. But mankind could not foresee the possibilities of using these technologies, putting telecommunications and global computer networks at its service. Today, not only people, but also entire countries can become victims of criminals operating in virtual space. At the same time, the safety of thousands of users may depend on a few criminals. The number of crimes committed in cyberspace is increasing in proportion to the number of users of computer networks, and according to Interpol estimates, the rate of increase in crime. Since the problem of cybercrime is global in nature, it cannot be limited to one country, so it requires serious and large-scale research, as well as the development of uniform international standards - from conceptual apparatus to uniform legal norms. In this work, we use the definition of "cybercrime" that meets international standards. The term "computer crime" used in local literature for illegal activities using computer technologies does not accurately reflect the nature of this phenomenon, which leads to the fact that the term "computer crime" means a much wider range of actions than what is described below.

Cybercrime is much broader in nature than computer crime and includes a range of illegal acts. In this work, cybercrime means a set of crimes committed in cyberspace, computer systems or computer networks, as well as other means of accessing cyberspace, computer systems or networks, and against computer systems, computer networks, and computer data.

Western European Journal of Linguistics and Education
Volume 2, Issue 7, July, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed

Accordingly, cybercrime means illegal interference with the operation of computers, computer programs, computer networks, unauthorized modification of computer data, as well as other illegal activities committed with or through computers, computer networks and programs, as well as through them. Socially dangerous behavior is understood. other input devices to the computer-simulated information space.

Cyber law is a field of law aimed at regulating and protecting relationships in the field of information, information resources and information system use. Therefore, cyber law should be considered as an element of the new legal system, which is expressed among other areas of law. This, in turn, requires clarifying the relations regulated by this legal network, their object, subjects, and the rights and obligations of subjects. The subject of legal regulation of cyber law includes a set or sum of social relations that occur in cyberspace and are regulated by the norms of various legal fields.

Informatization of production values of our country is a natural continuation of objective process of society development and collection, storage, transmission, processing and presentation of necessary information. Improving the quality of work, labor productivity and efficiency in the fields of economy, production, communication, scientific research, education, medicine and business is connected with the most modern information and communication technologies applied in them. Modern information and communication technologies deliver collected information products to people at a rapid pace and create wide opportunities for solving existing problems while reducing the level of labor. Therefore, the effective use of information and communication technologies in all sectors of the economy serves as an indicator of the technological and economic development of the country.

RESEARCH METHODOLOGY:

Cyber law information exchange includes the development of software and the operation of Internet resources. In other words, cyber law, as a branch of legal science, claims to study all the legal relations that exist in an integral connection with computer technologies and/or virtual space. Article 1158 of the Civil Code of the Republic of Uzbekistan can be supplemented with the following provision: is determined on the basis of the manifestation of the legal relationship with the legal order of more than one country".

Cyber law or IT law is called Internet law. Cyber-law is defined as a legal system designed to address the Internet, computing, cyberspace, and related legal issues. The Right Introduction to Cyber Law: It's 'Paper Laws' in a 'Paperless World'. Cyber law includes aspects of intellectual property, contract, jurisdiction, data protection laws, privacy and freedom of expression. It manages the digital revolution of software, information, online security and e-commerce. The field of cyber law provides legal recognition of electronic documents. It also creates a framework for e-commerce transactions and e-replenishment. So, to understand the meaning of Cyber law, it is the legal infrastructure to fight against Cyber Crimes. The increasing use of e-commerce makes it important to establish appropriate regulatory practices to prevent violations. Applicable cyber security laws vary widely from country to country and their respective jurisdictions. Similar penalties vary from fines to imprisonment depending on the crime committed. It is important for citizens to know their country's cyber laws to ensure that they are familiar with all information related to cyber security. The Computer Fraud and Abuse Act of 1986 was the first cyber law in existence, prohibiting unauthorized access to computers and illegal use of digital data. Since any crime creates a series of changes in the environment where it was committed, which are called traces in forensic science, there is a need to use virtual (or digital) traces to detect and investigate cyber crimes. In this regard, in

Western European Journal of Linguistics and Education
Volume 2, Issue 7, July, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed

criminology, a new direction of studying crimes committed using high information technologies has emerged and is developing. It is known that traces are divided into material and ideal according to the type of their carrier as a source of information of forensic importance. Material traces result from the interaction of the subject or object with elements of the material environment (hand and shoe prints, biological traces, bullets and cartridges, etc.). Ideal traces reflect the objective reality related to the crime event in the mind of a person and are stored in his memory in the form of images formed in the process of perceiving the event. The role of virtual traces in the generally accepted forensic classification is not fully defined. In specialized literature, different opinions are expressed about the place and role of these traces in forensic examination. First of all, digital information carriers are tangible objects with certain physical properties (for example, hard disks, flash cards, etc.).

On the other hand, digital information is the result of the mental activity of a certain person, it can be determined only with the help of special technical devices, and its study requires special knowledge. In this regard, it can be noted that virtual traces from a forensic point of view have a dual nature and can be divided into a separate category used in the detection and investigation of cybercrimes.

The second problem is related to the high latency of cybercrimes and the fragility of virtual traces. This type of offense is characterized by dynamic methods and can be committed from multiple locations using multiple devices at the same time. Victims do not always contact the law enforcement authorities in time to report the crime, which leads to the loss of relevant digital data, because criminals can destroy virtual traces: delete the account used in the commission of the crime , change the IP address of the device. , disable or destroy the device, cash out or delete stolen funds from the network, etc. In addition, it is difficult to obtain forensically relevant information because the retention periods in the network are determined at the discretion of the provider and are not regulated as in some foreign countries. In addition, the digital information found can only be removed by copying, which does not ensure its safety in its original form and results in the loss of the original date and time of creation. The absence of relevant legal norms in the current criminal procedural legislation may lead to recognition of copied information as unreliable evidence in the case, since such evidence was not obtained from procedural sources, but through procedural means.

Cybercrime is a new, understudied type of crime committed using information technology. Currently, activities in the legal Internet space in Russia are practically not regulated at the legislative level. In addition, in addition to the public part of the World Wide Web, there is also the "deep Internet", which is a platform for committing various crimes, from selling drugs to distributing child pornography. In this regard, another problem arises: the fight against cybercrime is complicated by the fact that the subjects of forensic activity do not have practical experience in detecting and investigating this category of crimes, as well as they do not have special knowledge in the field of information technologies. To solve investigative problems, law enforcement agencies often use the help of experts from cybercrime prevention and investigation companies. For example, specialists of the Russian company Group-IB are engaged in procedural actions and rapid search activities for collecting virtual traces and obtaining evidence, participating in court proceedings. However, despite these problems, electronic data is actively used as evidence in criminal proceedings. We remind you that in accordance with the current criminal procedural legislation, the evidence obtained in this way is considered physical evidence or other documents. In addition, the content of the concept of "digital evidence" is not established in any legal document.

Western European Journal of Linguistics and Education
Volume 2, Issue 7, July, 2024
https://westerneuropeanstudies.com/index.php/2
ISSN (E): 2942-190X Open Access| Peer Reviewed

Conclusion: In our opinion, in order to increase the effectiveness of the use of virtual traces for the purpose of searching and identifying evidence in criminal cases, it is necessary to establish the rules for their collection, research and evaluation at the legislative level. This requirement is due to the fact that virtual traces are intangible, so their identification requires special knowledge in the field of information technology. In addition, virtual traces, unlike traditional traces, are much easier to change and destroy, so the timeliness of their detection and research using special knowledge in the field of information technology and technical and forensic tools efficiency is of great importance. and cybercrime investigations. Simply copying the identified digital data into the relevant media can have a significant impact on the discovery of the true circumstances of a criminal case.

The use of virtual traces as a source of digital evidence in the investigation process is one of the most promising directions, and the development of forensic methods of cybercrime investigation allows to successfully solve the listed problems. In order to increase the effectiveness of combating cybercrimes, it is appropriate to actively develop criminalistics as one of the branches of forensic technology. The main focus should be on the development of techniques, methods and tools for the collection and examination of virtual traces to obtain digital evidence in the investigation and prosecution of computer crimes. A competent approach to conducting investigative actions and rapid search activities to obtain digital evidence allows not only to determine the factual circumstances of a cybercrime incident and expose criminals, but also to determine the causes of cybercrimes. In this regard, targeted training of specialists in the field of combating cybercrime is important for law enforcement agencies.

References:

1. Buz S.I. Kiberjinoyatlar: tushunchasi, mohiyati va umumiy xususiyatlari. URL: https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-suschnost-i-obschaya-harakteristika/viewer.
2. Jinoyat kodeksi 1996 yil 13 iyundagi 63-F3-son (2021 yil 1 iyulda kiritilgan o‘zgartirish va qo‘shimchalar bilan 2021 yil 1 dekabrdan kuchga kirgan [Elektron resurs]. SPS-dan kirish "ConsultantPlus" ".
3. Vexov V.B. Elektron dalillarni qayd etish tushunchasi, turlari va xususiyatlari // Jinoyatlarni tergov qilish: muammolar va ularni hal qilish yo‘llari: ilmiy va amaliy ishlar to‘plami. ishlaydi M., 2016 yil. 1-son.
4. Zigura N.A. Kompyuter ma'lumotlari Rossiyada jinoyat protsessida dalil turi sifatida: mavhum. dis. ...kand. qonuniy Sci. Chelyabinsk, 2010 yil.
5. Rossiya Federatsiyasining 18 dekabrdagi Jinoyat-protsessual kodeksi. 2001 yil 174-FZ-son (2021 yil 1 iyul, 2021 yil 23 sentyabrdagi o‘zgartirishlar bilan) // SZ RF. 2001 yil. 52-son (I qism). Art. 4921.
6. Vershitskaya G.V., Zyabina A.S., Kudasheva K.A. Biometrik identifikatsiya texnologiyasi: yuzni aniqlash tizimi // Raqamli kelajak: biz yashaymiz!: ilmiy maqolalar to‘plami. Saratov, 2021. 185-191-betlar.
7. Askolskaya N.D. Virtual izlar kompyuter jinoyatlarining sud-tibbiy xususiyatlarining elementi sifatida.
URL:https://cyberleninka.ru/artide/n/virtualnye-sle-dy-kak-element-kriminalisticheskoy-harakteristiki-kompyuternyh-prestupleniy/viewer.