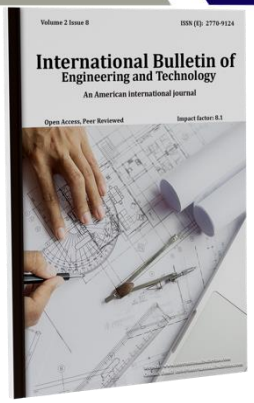

THE CONCEPT, CLASSIFICATION, AND QUANTITATIVE AND QUALITATIVE INDICATORS OF CYBERSPATIAL FRAUD

Bakhtiyorov Ikhtiyor Bakhtiyor ugli
Master's student of the University of Public Security of the Republic of Uzbekistan, Captain
E-mail:ibaxtiyorov2007@gmail.com
https://doi.org/10.5281/zenodo.17223620

Abstract. This article scientifically analyzes the formation of the concept of cyberspace, the concept of fraud committed within it, its main features, their classification according to various forms and methods of commission, as well as quantitative and qualitative indicators of fraud crimes committed in cyberspace.

Keywords: cyberspace, cyber fraud, phishing, vishing, inheritance fraud, international mail scams, phishing contests, internet begging, online store fraud, marriage fraud, freelance services, malware, crypto fraud.

Introduction

In recent decades, technological progress has transformed almost all aspects of society. The Internet and information and communication technologies have become an integral necessity in people's daily activities. As a result, a new phenomenon called "cyberspace" has emerged. Cyberspace is a complex system that encompasses not only technological processes, but also social, economic, political, and cultural relations. Today, studying the content and essence of cyberspace is relevant for two main reasons: firstly, it creates new opportunities for the development of society; secondly, it serves as a platform for cybercrime and various threats.

Formation of the concept of cyberspace. The term "cyberspace" was first mentioned in the story "Burning Chrome" by American writer William Gibson, published in "OMNI" magazine in 1982, and was used as a term in Gibson's science fiction novel "Neuromancer." Today, the internet and digital technologies have become an integral part of our lives. These technologies, on the one hand, make life easier, and on the other hand, give rise to new types of crimes, particularly cyber fraud.

Cyber fraud has become especially widespread throughout the world, evolving into a type of crime that causes significant economic and social damage. Fraud committed in cyberspace has its own peculiarities, as it is characterized by speed, anonymity, and a global nature.

The concept of cyber fraud. The term "computer fraud" (computer fraud) appeared in the 70s of the last century and has been the subject of much debate among scientists to this day. In particular, D.A. Ziykov put forward the concept of computer fraud as "the seizure of another's property or the right to another's property through deception or abuse of trust using computer technology"[1]. M.A. Yefremova believes that cyber fraud and computer fraud are the same concept, that is, synonyms[2]. Professor N.A. Lopashenko defines computer fraud as fraud related to the use of computer technologies to obtain non-cash funds and non-documentary securities[3].

Main features of cyber fraud: use of the Internet and digital technologies - cyber fraud is usually carried out through the Internet, computers, mobile devices, and other digital technologies. Anonymity - cyber fraudsters can hide themselves using the anonymity of the Internet, which makes it difficult to identify and punish them. Global character - a crime that can be committed in all countries via the Internet. Speed and efficiency - Fraud can be committed in a short time and their impact can be very significant. Because easy access - the ability to access the internet and digital systems - is widespread, scammers can attack in various ways: using fake online stores, fake applications, or social engineering methods. In addition, cyber fraud is one of the most difficult crimes to solve, differing from other types of crimes in its thorough planning, extreme complexity, and transboundary nature.

Cybercrimes, including fraud, theft of financial information, the dissemination of malicious programs, and information manipulation, are becoming widespread. This creates the need for legal regulation of cyberspace and its transformation into a safe environment. In the regulation of cyberspace in the Republic of Uzbekistan, the norms established in the relevant articles of the Law "On Cybersecurity," the Criminal Code, and the Code of Administrative Offenses, in particular, Chapter 201 of the Criminal Code, entitled "Crimes in the Field of Information Technologies[4]," as well as special state programs ensuring cybersecurity, are of great importance.

By the Decree of the President of the Republic of Uzbekistan dated January 28, 2022 No. UP-60 "On the Development Strategy of New Uzbekistan for 2022-2026," a number of tasks were defined for monitoring investigative activities, reforming operational-search activities to solve new types of crimes committed using information technologies, including cybercrimes, attracting additional forces and resources, and further increasing the effectiveness of protecting the dignity and freedoms of citizens in the process of combating these crimes[5].

Classification of cyber fraud by methods of its commission:

Phishing is one of the methods of committing a fraudulent crime related to bank cards; it is a method of "phishing," i.e., "fishing." In this case, fraudsters with sufficient knowledge and skills in the field of IT technologies gain the user's trust and seize confidential bank card information[6]. The peculiarity of the method of committing a crime is that the perpetrator sends an SMS message to the user's social network account, email, or mobile communication devices through remote means of communication or fake web pages. Social engineering methods are used in this process. We will provide a detailed explanation of this below.

Criminal groups engaged in "phishing" send notifications in various forms requesting the victim to enter their personal data. The victim believes that they are accessing the bank's official website to use banking services. In particular, by entering their full name, card details, and PIN code on a fake website, they unknowingly fall prey to "phishing" operators[7]. Creating fake websites is one of the modern methods of phishing. Detecting such phishing sites without special knowledge and skills is very difficult.

Vishing - one of the most common fraud methods in our country today is online Vishing fraud. In this method of fraud, scammers obtain their "prey" by phone. The word "vising" comes from English, that is, from the combination of the words "voice" - "voice" and "fishing" - "fishing"[8]. In this fraudulent method, fraudsters obtain confidential SMS information sent to them from victims through various lies and fabrications, identifying themselves as bank employees, payment system employees, or similar.

In our country, such cases have sharply increased, in particular, fraudsters, introducing themselves as "Click or another payment system employee," by deceiving and gaining the trust of citizens, as if to correct some shortcomings in the system and eliminate payment-related shortcomings, send an SMS to the victim and ask him to tell the code number indicated in the SMS message. As soon as the code number indicated in the SMS message is called, the funds are transferred to various plastic cards or phone numbers, transferred to the Qiwi wallet via Click, and the criminally recovered funds (soums) are converted into foreign currency.

Inheritance fraud - a message about leaving a large inheritance in the name of a victim from a relative abroad is reported under the guise of his lawyer. After this, confidential information about passport and plastic card numbers is fraudulently confiscated for the registration of inheritance and making initial payments.

International postal items - the recipient is sent a certain type of valuable cargo, a label of various postal items for payment of postal expenses for receipt, or photographs confirming that the item is in their name. In this way, confidential information about the plastic card number is obtained by deception.

Phishing competitions - the organization of fake competitions on social networks. In this case, a vehicle or the latest phone is awarded as a prize. It is noteworthy that the organizers send messages to almost all participants, congratulating them on a win, such as "You won the lottery, or participate in a limited number of prizes, get a prize," or encouraging them to participate in the competition. Usually, participants of a phishing competition understand that this process is fraud after participating in the competition several times.

Internet begging - the posting of photographs of persons suffering from various diseases or in a difficult situation on the websites of fake charitable foundations and on social networks, asking for material assistance on their behalf. Fraudsters focus more on methods of psychological influence that evoke feelings of humanity, compassion, and trust. Usually, the individuals whose names are being announced do not have any information about the accumulation of funds for them. The reason is that any donated funds are transferred directly to the accounts of fraudsters.

Fraud related to online stores - some scammers deceive customers by selling counterfeit, low-quality goods or products, while others require partial or full prepayment for the product[9]. After payment is made, the goods will not be delivered to the buyer.

In recent years, there has been an increase in fraud related to online stores in our country. In particular, there are cases of withdrawal of funds from bank plastic cards in trades currently carried out through the online platform "OLX.uz."

Fraudsters, citing being in another region or abroad, deceptively ask the victim to give the bank card number and the code indicated in the SMS message to pay for the goods planned for purchase. After this, work is carried out according to the above procedure.

Marital fraud - using photographs of other people on social networks, correspondence with victims on their behalf and gaining their trust. Over time, after requesting financial assistance from the victims and receiving the intended funds, the account will be deleted.

Freelance services are the provision of online services to the client in the form of creating a website, writing articles, translation work, advertising logos, videos, etc. in exchange for an agreed service. The essence of this method is manifested in the fact that the

victim (freelancer) sends an order to the customer (fraudster) and the criminal disappears without paying the agreed amount.

Malware (Malicious Software) - scammers steal personal data by deceiving users by installing malware on their devices.

Crypto-fraud: Fraud committed with cryptocurrencies, such as counterfeit crypto-communications.

Quantitative and qualitative indicators of fraud committed in cyberspace.

According to analyses and statistics, the annual global damage from cybercrime in 2024 amounted to 11.4 trillion dollars. In the context of globalization and digitalization, crimes committed using digital technologies are increasing year by year, and the transformation of traditional crimes into cybercrimes is also expanding in our country. In particular, over the past five years, cybercrimes in our country have increased 68 times, and in the past year alone, compared to 2023, they have increased by 9.1 times. During this period, the number of appeals received from individuals and legal entities regarding offenses in cyberspace increased 34 times. As a result of these crimes, more than 1 trillion 909 billion soums of citizens' funds were embezzled. If in 2019 863 crimes of 18 types were committed through information technologies, then in 2024 58,800 crimes of 62 types were registered, and a significant increase in the share of cybercrimes in the total crime is observed, which makes the need for their prevention even more urgent. In 2023, the share of cybercrime in total crime was 6.2 percent, in 2024 it reached 44.4 percent, and almost every other crime was committed through information technology. This situation requires the continuous improvement of the prevention system year after year. The main part of cybercrimes (98 percent) consists of crimes related to bank cards (cyber theft and cyber fraud).

Cybercrimes are mainly committed in the following ways:

- 60 percent by sending malicious links and programs;
- by acquiring control of a bank card or mobile device;
- 16 percent - by obtaining SMS codes confirming the management of bank cards and accounts in mobile applications through various deceptions;
- 4 percent through online loan registration in the name of a person;
- 11% through fraud on online trading platforms;
- 9 percent are committed in the form of attracting citizens' funds through various fraudulent schemes.[10]

In accordance with the resolution "On Measures Aimed at Further Strengthening Activities to Combat Crimes Committed with the Help of Information Technologies," the following measures have been established for the early prevention of cybercrime:

Firstly, in order to strengthen the responsibility of banks and payment organizations for complying with their information security policy and cybersecurity requirements, the Ministry of Internal Affairs will introduce the practice of publishing a list of banks and payment organizations with the highest number of registered cybercrimes (resulting from vulnerabilities and shortcomings) at the end of each month.

This will encourage banks and payment organizations to take serious measures to strengthen their security systems, and citizens will have the opportunity to identify and choose banks and payment applications with a robust protection system.

Secondly, the Central Bank will establish a system for identifying and promptly reporting to law enforcement agencies instances of signs or suspicions of fraudulent schemes

aimed at attracting public funds ("financial pyramids") through monitoring transactions of individuals and legal entities.

In this case, the Central Bank will develop a mechanism for detecting suspicious transfers, and the information will be sent to the Ministry of Internal Affairs through an electronic data exchange system. As a result, early prevention of cases of investing in fraudulent schemes and being deceived by citizens will be ensured.

Thirdly, the Cabinet of Ministers annually approves a comprehensive propaganda program aimed at improving the population's cyberculture and forming cyber hygiene, and the month of November is declared "Cyber Culture Development Month" at the republican level.

After all, due to insufficient cyber literacy, citizens themselves provide their personal data to fraudsters or download malicious programs from social networks.

Fourthly, based on requests from responsible departments of internal affairs bodies, the practice of promptly blocking bank cards related to suspicious money transfer operations will be introduced. As a result, it becomes possible to return 80% of the money embezzled through fraudulent crimes, including "financial pyramids," to their owners.

Fifthly, a procedure will be established for the free use of targeted advertising services on the Internet and social networks to warn about the forms of cybercrimes and the methods of their commission.

Today, it is observed that young people spend most of their time on social networks and promote ideas alien to our national values. Although targeted advertising on the Internet is costly, it is proving to be effective.

Sixthly, banks will establish the practice of informing parents about suspicious (fraud) transactions related to their minor children. This will serve to reduce the proportion of minors falling into the trap of fraudsters.

Seventhly, information about bank cards related to suspicious money transfer operations will be immediately provided to the responsible departments of internal affairs bodies, and a register (drop) of persons to whom citizens have provided information on their bank accounts, bank cards, and electronic wallets for committing cybercrimes will be maintained[11].

In conclusion, it should be noted that this article analyzes in detail the concept of cyberspace, the essence and main features of fraud committed in it, as well as quantitative and qualitative indicators. President of the Republic of Uzbekistan Sh. MIRZIYOYEV Mirziyoyev's statement at the 80th session of the UN General Assembly that..."preventing inequality between countries in the use of digital development and artificial intelligence is very important"12" shows that one of the urgent problems today is the need for everyone to be vigilant and aware, to be able to analyze information in order to combat cybercrime in the process of increasing globalization.

References:

1.Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества. Владимир, 2002. – 211 с.

2.Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. № 4. С. 19-21.

3.Лопашенко Н.А. Посягательства на собственность: монография. – М.: Норма, Инфра-М, 2012. – С. 8.
4.O‘zbekiston Respublikasining Jinoyat kodeksi.
5.2022 yil 28 yanvardagi O‘zbekiston Respublikasi Prezidentining «Yangi O‘zbekistonning 2022–2026- yillarga mo‘ljallangan taraqqiyot strategiyasi to‘g‘risida»gi PF–60-son Farmoni.
6.Шаззо С.К. Способы совершения мошенничества в отношении граждан. Вестник Адыгейского государственного университета. Серия 1: Юриспруденция» 2008, № 2, стр. 5.
7.Изотов Д. С., Бикова Н. Н. Виды мошенничества с банковскими картами [See bank card fraud]. Вестник НГИЭИ. 2015. – № 3. – С. 49-52.
8.Табак И.С. Мошенничество с банковскими картами / И.С. Табак // Современные инновации. – 2018. – № 4 (26). – № 1 (19). – С. 37-40.
9.Козодаева О. Н., Обиденнова А. С. Способы совершения мошенничества с использованием банковских карт [Ways to commit fraud using bank cards]. Учёные записки Тамбовского отделения РоСМУ. С. 52
10.Toshpo‘latov A.A. Kiberjinoyatlarni jilovlash orqali xavfsiz kibermakon yaratish.Raqamli transformatsiya sharoitida kiberjinoyatlarning barvaqt oldini olishda O‘zbekiston tajribasi. “Yangi O‘zbekiston” gazetasi 07.05.2025 yil №92-son –1-3 c.
11.2025-yil 30-apreldagi O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qarori.
12.2025-yil 23-sentyabrdagi O‘zbekiston Respublikasi Prezidenti Sh. Mirziyoyevning BMT Bosh Assambleyasining 80-sessiyasidagi nutqi.