SOME CONSIDERATIONS ON IMPROVING CYBERCRIME PREVENTION

Shodmonov Ubaydullohon Turakhujaevich
Senior lecturer of the Department of Fundamental Economic Sciences at the ISFT (International School of Finance, Technology and Science)
https://doi.org/10.5281/zenodo.14760029

Abstract: This article thoroughly examines the experiences of foreign countries in improving cybercrime prevention, as well as the opinions and views of foreign scholars who have conducted research in this field. The author has developed proposals and recommendations based on this analysis.

Keywords: cybercrime, internet, online services, prevention, phishing.

Today, cybercrime, specifically fraud committed through the internet, poses a serious threat to all countries worldwide. With the development of the Internet and the expansion of digital technologies and online services, the number of cybercrimes is increasing. The problems of preventing and combating cybercrime are particularly relevant, as thousands of people fall victim to this type of crime every year. The prevention of cybercrime, that is, measures aimed at its prevention and reduction, is of great importance in scientific research and practice worldwide today. In this article, we will examine existing problems in this area and ways to solve them by analyzing the main scientific approaches to improving cybercrime prevention, the opinions of scholars, best foreign practices, and the current situation in Uzbekistan.

Cybercrime refers to various types of fraud that are carried out using the Internet, computer networks, and digital technologies. The most common types are[1]:

- Phishing (stealing user information): Scammers fraudulently obtain users' personal information, passwords, and bank account information over the Internet.

Ransomware (Blackmail Software): Cybercriminals block computer systems and demand a certain amount of money from the user.

- Fraud through online sales and purchases: Engaging users into fake online stores and getting money from them.

Identity theft: Cybercriminals commit fraud on behalf of others by stealing their personal information.

The development of cyber fraud is driven by the widespread use of the internet, the availability of technologies that ensure anonymity, and legal gaps. New technologies and innovations, such as artificial intelligence, databases and digital currencies, are also creating new forms of cyber fraud.

There are various scientific approaches to preventing cyber fraud. First and foremost, scientists emphasize the need to enhance cybersecurity and strengthen legal norms. For example, according to the principle of "layer approach to cybersecurity," developed by scientists, the fight against cyber fraud should not be limited to technical measures only in the first layer. Instead, it is important to implement security at multiple levels, i.e. to combine technological, legal, social, and educational measures.[2]

Japanese scientist Yoshitaka Ikeda (2020) proposed several strategies to strengthen the prevention of cyber fraud. In his opinion, it is necessary to develop a "security culture" for each user and organization. This included: regular cybersecurity trainings, training in safe online behavior rules, data encryption, and improvements to online identification systems.[3]

In addition, scientists consider it important to develop cyber fraud detection systems using "artificial intelligence" technologies. In particular, as a result of scientific research in Central Asia and Europe, artificial intelligence and machine learning algorithms are being used to detect unwanted actions in databases. These systems allow real-time user activity monitoring and detection of any suspicious activity.

There are various successful experiences in combating cyber fraud abroad. For example, in America, many laws and norms have been developed in the field of cybersecurity. The Sarbanes-Oxley Act, enacted in 2002, mandates companies and organizations to ensure the security of their data.[4] This law requires organizations to define cybersecurity strategies and report annually.

The European Union introduced the "General Data Protection Regulation" (GDPR) in 2018. This regulation, aimed at protecting the data of not only legal entities, but also individuals, created new approaches to combating cyber fraud. GDPR also includes strengthening cooperation between information technology and law enforcement agencies in ensuring the security of personal data on the Internet.

Cybersecurity and cyber fraud prevention measures in Uzbekistan have significantly improved in recent years. This can also be seen in the adoption of the Law of the Republic of Uzbekistan "On Cybersecurity" [5] in 2022. This law defined the state's approach to cybersecurity and placed a responsibility on government agencies, the private sector, and citizens to create a safe and reliable internet environment.

In addition, the government of Uzbekistan has implemented numerous reforms to introduce national standards and security systems in the field of data protection to ensure cybersecurity. Currently, special trainings and seminars on cybersecurity are being held in Uzbekistan, which serves to further strengthen the process of combating cyber fraud in the country.

The prevention of cyber fraud is an important task for all countries today. According to scientists, cybersecurity should not be limited to technical measures. Instead, it is important to develop a cybersecurity culture, enlighten users, and use cutting-edge technologies such as artificial intelligence to detect cyber fraud. The use of foreign experience, as well as the reforms being implemented in Uzbekistan, serve as effective tools for preventing cyber fraud. Cybersecurity can be further strengthened through cooperation, the application of knowledge and technologies in the fight against cyber fraud. In conclusion, it is necessary to put forward the following proposals aimed at improving the prevention of cyber fraud, which is currently recognized as a highly dangerous "plague":

From the perspective of developing a cybersecurity culture, it is important to develop a conscious approach to cybersecurity in every citizen and organization, teaching and widely promoting the basic rules of safe online behavior. This will create a strong and unified system to combat cyber fraud in society.

As a measure aimed at wider use of technologies and artificial intelligence, the introduction of artificial intelligence and machine learning algorithms to detect and combat

cyber fraud serves as an effective tool for real-time detection of dangerous actions.
These technologies play an important role in strengthening cybersecurity and preventing fraud.

From the perspective of strengthening the legal framework for combating cybercrime, it is necessary to improve the legal framework to prevent cyber fraud and ensure its effective prevention. This can be done, in particular, by developing laws that comply with international standards for data protection, personal data storage, and cybersecurity.
It is necessary to ensure effective cooperation between the state, the private sector, and civil society in combating cyber fraud.

References:

1.Кибермошенничество: виды и способы обмана в Интернете. https://cbsykt.ru/news/kibermoshennichestvo-vidy-i-sposoby-obmana-v-internete/
2.Расулев А.К. Перспективы правовой политики в области противодействия киберпреступности в Узбекистане. https://illp.uz.
3.Подходы Японии к кибербезопасности на примере сотрудничества с АСЕАН. https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/podkhody-yaponii-k-kiberbezopasnosti-na-primere-sotrudnichestva-s-asean/
4.Что такое соблюдение Закона Сарбейнса-Оксли (SOX)?. https://continuumgrc.com/ru/what-is-sarbanes-oxley-act-sox-compliance/.
5.O‘zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O‘RQ-764-son. https://lex.uz/uz/docs/-5960604