Western European Journal of Historical Events and Social Science
Volume 04, Issue 05, May 2026
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

MODERN TRENDS IN CYBERFRAUD CRIMES COMMITTED THROUGH INFORMATION TECHNOLOGIES AND ISSUES OF THEIR QUALIFICATION.

Xolboyev Shohruhjon Olimjonovich Independent Researcher of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract: This article analyzes the modern manifestations of cyber fraud, in particular, the social danger of financial crimes committed using the Internet and information and communication technologies, the mechanisms of their commission, and the issues of legal regulation. The study highlights the negative impact of cyber fraud on the banking system, electronic payment instruments, and information systems, and reveals the role of information systems and digital technologies of internal affairs bodies in preventing these crimes.
Keywords: cyber fraud, cybercrime, information technology, information security, digital evidence, internet fraud, bank cards, electronic payment system, information and communication technologies.

The crime of falsifying deposits via the Internet or special technical devices is also a type of cyber fraud, which, although rare in practice, is considered a very large and devastating crime in terms of the risk of harm. This crime is mainly committed by bank employees or employees responsible for transferring funds from one account to another, and this crime concerns the actions of these employees to keep money for themselves instead of depositing it into a customer's account. In this case, banks design their business processes in a way that minimizes fraud, but this crime is committed as a result of mutual agreement between employees who are connected to each other.

In the case of abuse of trust, the user, in order to increase his funds, entrusts the funds to the custodian, based on his own will, and the custodian, using information technologies and communications, acquires the entrusted property or property rights.

The object of cyber fraud, like the object of fraud, is another person's property or property rights.

Considering that these crimes are distinguished by their broad scope and the fact that such crimes can cause great harm, we consider it appropriate to establish liability for these crimes in a separate article in our criminal legislation.

As we can see, the concept of cyberfraud crime and responsibility for it are not defined in our criminal law, it is appropriate to establish responsibility for this category of crimes in our criminal law in order to show that punishment is inevitable for persons who commit socially dangerous acts in this regard and to ensure that the rights of owners are guaranteed.

Taking into account the fact that currently, in order to hold a person who has committed a socially dangerous act accountable, liability for such crimes is not established and any act not prohibited by law is not considered a crime, and taking into account the above-mentioned foreign experience, it is proposed to remove paragraph "c" of part two of Article 168 of the

Western European Journal of Historical Events and Social Science
Volume 04, Issue 05, May 2026
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

current Criminal Code from [1]this Code by adding an additional article to Article 169 of the Criminal Code for cyber fraud or a separate article to the Criminal Code being developed in a new edition in accordance with the Resolution of the President of the Republic of Uzbekistan No. PP-3723 dated May 14, 2018 "On measures to radically improve the system of criminal and criminal procedural legislation".

Due to the lack of criminal liability for cyber fraud, there are still many problems in this area, and the lack of an appropriate explanation from the Plenum of the Supreme Court makes it difficult to find a solution to these problems. It is proposed that the Plenum of the Supreme Court adopt a decision on the inclusion of this crime in the criminal legislation in this area, and that this Plenum should discuss the distinctive features of these crimes from other fraud crimes, the types of these crimes, the forms and methods of their commission, the specific aspects of their detection and qualification, as well as the expediency of determining the punishment and liability measures for these crimes, and the subject and object of these crimes.

Information technology is the main organizer of organizational management information systems, which is directly related to the specific features of the work of internal affairs departments . In internal affairs bodies e l ect r o n h u jj a t a y la ni sh i t i z i mi n i j o r i y et i sh v a special [2]attention is paid to profit .

There are common and distinctive features inherent in the work of management activities in internal affairs bodies and employees directly involved in the prevention, detection and investigation of crimes, maintaining public order, and the rehabilitation of convicts. These are the collection, processing, and analysis of information, and the development of various management decisions based on them to achieve the goals set for the system.

The assessment of the emergency situation is closely related to the completeness and correctness of the decisions being made, the direction of the action according to the plan, the clarity and precision of the task assigned to the executor, the effectiveness of control and crime detection, and the quantity and reliability of information.

For the use of operatives serving in the internal affairs bodies, a database network called the “Integrated Information Bank of Uzbekistan” is operating in the Information Center of the Ministry of Internal Affairs of the Republic of Uzbekistan. This network contains information on wanted and missing persons, registered and wanted vehicles, stolen or lost weapons, lost digital items, and telephone numbers throughout the republic and the CIS countries. This system internal affairs corporate computer network in the bodies expansion and from it use provides .

Information Centers in regional internal affairs departments operate in several areas. In particular, the statistics group analyzes daily incidents and crimes committed in the region. Any information of interest to internal affairs bodies can be found in the database of this service. Therefore, an integral connection and connection have been established between the activities

[1] Ўзбекистон Республикаси Президентининг “Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида” 2018 йил 14 майдаги ПҚ–3723-сон қарори // Қонун ҳужжатлари маълумотлари миллий базаси, 15.05.2018 й., 07/18/3723/1225-сон, 01.10.2018 й., 06/18/5547/1975-сон. 309

[2] Ўзбекистон Республикаси Ички ишлар Вазирининг “Ички ишлар органларида электрон ҳужжат айланиши тизимини жорий этиш ва фойдаланиш тартиби тўғрисидаги йўриқномани тасдиқлаш ҳақида”ги 2015 йил 19 апрель 64 – сон буйруғи.

Western European Journal of Historical Events and Social Science
Volume 04, Issue 05, May 2026
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

of employees of this service and the activities of other departments of internal affairs bodies. Because this is where information is recorded on the number of all types of crimes, previously convicted citizens, places of residence of drug dealers, hijacking of transport, assault, robbery and other types of crimes.

The program of comprehensive measures for radical reform of the system of internal affairs bodies, which includes priority directions, stipulates the introduction of modern information and communication technologies to the activities of internal affairs bodies [3].

This, in turn, creates the need to pay serious attention to protecting people from Internet attacks, promoting a culture of receiving and distributing information, and ensuring network security. According to the international Internet security organization Symantec Security, currently one in 12 people in the world falls victim to an Internet attack every second, and more than 556 million cyberattacks are carried out annually, and the amount of damage suffered by victims is more than 100 billion US dollars [4].

List Of References Used

1 Ўзбекистон Республикаси Президентининг “Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида” 2018 йил 14 майдаги ПҚ–3723-сон қарори // Қонун ҳужжатлари маълумотлари миллий базаси, 15.05.2018 й., 07/18/3723/1225-сон, 01.10.2018 й., 06/18/5547/1975-сон. 309

2.Ўзбекистон Республикаси Ички ишлар Вазирининг “Ички ишлар органларида электрон ҳужжат айланиши тизимини жорий этиш ва фойдаланиш тартиби тўғрисидаги йўриқномани тасдиқлаш ҳақида”ги 2015 йил 19 апрель 64 – сон буйруғи.

3.Ўзбекистон Республикаси Президентининг “Ички ишлар органларининг фаолияти самарадорлигини тубдан ошириш, жамоат тартибини, фуқаролар ҳуқуқлари, эркинликлари ва қонуний манфаатларини ишончли ҳимоя қилишни таъминлашда уларнинг масъулиятини кучайтириш чора-тадбирлари тўғрисида”ги, 2017 йил 10 апрелдаги Фармони. http://Lex.uz.

4.А.Анорбоев, Р.Хурсанов. Кибержиноятлар хавфини бартараф этиш йўллари. Ҳуқуқий, илмий-амалий нашр. 5/2020. 25-27 бетлар. https://sud.uz/wp-content/uploads/2021/odilsudlov/5_uz.pdf.

[3] Ўзбекистон Республикаси Президентининг “Ички ишлар органларининг фаолияти самарадорлигини тубдан ошириш, жамоат тартибини, фуқаролар ҳуқуқлари, эркинликлари ва қонуний манфаатларини ишончли ҳимоя қилишни таъминлашда уларнинг масъулиятини кучайтириш чора-тадбирлари тўғрисида”ги, 2017 йил 10 апрелдаги Фармони. http://Lex.uz.

[4] А.Анорбоев, Р.Хурсанов. Кибержиноятлар хавфини бартараф этиш йўллари. Ҳуқуқий, илмий-амалий нашр. 5/2020. 25-27 бетлар. https://sud.uz/wp-content/uploads/2021/odilsudlov/5_uz.pdf.