ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

STATE POLICY AND LEGAL APPROACH TO COMBATING CRIMES COMMITTED THROUGH INFORMATION TECHNOLOGIES: ANALYSIS AND PROPOSALS

Sh.S.Qosimov

Republic of Uzbekistan Research Institute of Criminology independent

researcher lieutenant colonel

Abstract: This article analyzes the dynamics of the increase in crimes committed using information technologies, the threats they pose to the security of society and the state, as well as the state policy and legal reforms implemented in Uzbekistan to counter such crimes. In particular, it examines the new institutional and legal mechanisms for combating cybercrime, developed based on the Presidential Decree No. ПҚ–153 dated April 30, 2025, the activities of authorized bodies, preventive measures, the responsibility of the banking and financial sector, and accountability measures. The article also offers specific recommendations for preventing these crimes and improving the legal framework.

Keywords:cybercrime, information technologies, legal reforms, prevention, ПҚ–153, cybersecurity, financial institutions, law enforcement agencies, digital security, crime prevention.

Аннотация:Мазкур мақолада ахборот технологиялари ёрдамида содир этилаётган жиноятларнинг ўсиш динамикаси, уларнинг жамият ва давлат хавфсизлигига таҳдиди ҳамда уларга қарши курашиш борасида Ўзбекистонда амалга оширилаётган давлат сиёсати ва ҳуқуқий ислоҳотлар таҳлил қилинган. Хусусан, 2025 йил 30 апрелда қабул қилинган ПҚ–153-сонли Президент қарори асосида кибержиноятчиликка қарши курашишнинг янги институционал ва ҳуқуқий механизмлари, ваколатли органлар фаолияти, профилактик тадбирлар, банк ва молия тизими масъулияти ҳамда жавобгарлик чоралари ёритилган. Шунингдек, ушбу жиноятларнинг олдини олиш ва ҳуқуқий базани такомиллаштириш бўйича аниқ таклифлар илгари сурилган.

Таянч сўзлар: кибержиноятчилик, ахборот технологиялари, ҳуқуқий ислоҳотлар, профилактика, ПҚ-153, киберхавфсизлик, молия ташкилотлари, ҳуқуқни муҳофаза қилувчи органлар, рақамли хавфсизлик, жиноятларни олдини олиш.

Аннотация:В данной статье проанализированы динамика роста преступлений, совершаемых с использованием информационных технологий, угрозы, которые они представляют для безопасности общества и государства, а также государственная политика и правовые реформы, проводимые в Узбекистане по противодействию таким преступлениям. В частности, рассматриваются новые институциональные и правовые механизмы борьбы с киберпреступностью, разработанные на основе Указа Президента № ПҚ–153 от 30 апреля 2025 года, деятельность уполномоченных органов, профилактические меры, ответственность банковско-финансового сектора и меры

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

привлечения к ответственности. Также предложены конкретные рекомендации по предупреждению данных преступлений и совершенствованию правовой базы.

Ключевые слова: киберпреступность, информационные технологии, правовые реформы, профилактика, ПК–153, кибербезопасность, финансовые учреждения, правоохранительные органы, цифровая безопасность, предупреждение преступлений.

In recent years, the rapid development of information and communication technologies has expanded the possibilities of using the Internet. This, along with accelerating the digitalization processes in all spheres of society's life and creating a number of conveniences, is also causing the emergence of new types of threats and risks. In the world, in particular, in Uzbekistan, the scale of crimes committed with the help of information technologies - cybercrime - is constantly expanding and poses a serious threat to the security of citizens, the state, and society.

A number of legal reforms are being carried out in Uzbekistan in order to combat these crimes, early detection and prevention of offenses. In particular, government decisions, legislative innovations, the activities of special agencies, and preventive measures carried out with the involvement of the public contribute to increasing the effectiveness of work in this area.

At the same time, official figures clearly demonstrate that cybercrime is a serious problem. In particular, during 2020-2024, the number of cybercrimes increased 68 times. Complaints about offenses in cyberspace have increased 34 times, and more than 1 trillion 909 billion soums of material damage has been caused to citizens. In 2019, 863 crimes of 18 types were registered, and in 2024, 58,800 crimes of 62 types were registered. In 2023, the share of cybercrime in total crime was 6.2 percent, and in 2024 this figure reached 44.4 percent. Of these, 98% are cybertheft and cyberfraud related to bank cards.

These data indicate the need to take measures to prevent cybercrimes, protect citizens from them, detect cyberattacks, and eliminate their consequences. In this process, the effective use of modern forms and methods is of great importance.

At the initiative of the President of the Republic of Uzbekistan Sh.M.Mirziyoyev, this issue was raised to the level of state policy, and the Resolution of the President of the Republic of Uzbekistan dated April 30, 2025 No. PP-153 "On Measures Aimed at Further Strengthening Activities to Combat Crimes Committed with the Help of Information Technologies" was adopted. This resolution is an important legal basis that allows us to approach the work in this area at a new level.

This resolution designates the Ministry of Internal Affairs as the authorized body for establishing a unified practice of combating cybercrime in the Republic of Uzbekistan, coordinating the activities of all responsible state bodies and institutions in this area, and organizing targeted cooperation.

In our country, there are specific sectoral laws to combat threats such as terrorism, extremism, illicit drug trafficking, human trafficking, corruption, and the legalization of criminal proceeds. However, there is still no comprehensive law of direct action that includes a legal description of cybercrime, its types, and liability measures. Therefore, in accordance with the task reflected in the resolution, the development of a separate draft law on the early prevention of cybercrimes and increasing the effectiveness of their detection, in particular, the development and adoption of a law on combating crimes committed by means of information technologies in the near future, is indicated as a priority task.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

In order to prevent cybercrimes and prevent citizens from becoming victims of these crimes, it is important to conduct legal awareness-raising work among the population. Taking this issue into account, the Resolution assigns strict responsibility to responsible state bodies, organizations, banks, payment system operators, and payment organizations for taking all necessary measures aimed at preventing cybercrime and raising the cyberculture of the population. It was instructed to amend the legislation to strengthen liability for non-compliance with cybersecurity requirements by legal entities, as well as for all crimes in the field of information technology. A procedure has been established for recovering material damage caused by cybercrimes committed as a result of non-compliance with the requirements of information security and cybersecurity of banks, payment systems, payment organizations, and other organizations.

According to statistics, the majority of cybercrimes related to bank cards are committed through bank cards issued in the name of another person. Therefore, the Presidential Decree provides for the establishment of administrative and criminal liability for persons who have issued a bank card in their name for the commission of a cybercrime. It was also determined that banks will establish a system for prompt notification of law enforcement agencies about suspicious transactions, and the Central Bank will develop a mechanism for identifying suspicious transfers, and this information will be sent to the Ministry of Internal Affairs through a data exchange system. These measures are aimed at preventing citizens from incurring financial losses by believing in fraudulent schemes based on promises of profit, informing them in advance, and ensuring their financial security.

In addition, this resolution introduces a number of mechanisms aimed at the early prevention of crimes. In particular, a list of banks and payment organizations with the highest number of cyberattacks will be published at the end of each month. The Central Bank will promptly inform the Ministry of Internal Affairs about the activities of financial pyramids.

The decree also stipulates that "Cyber Culture Development Month" will be held annually in November. These measures will become an effective means of preventing cybercrime by raising citizens' awareness of cybersecurity, forming a digital culture among young people, preventing crimes of this type, strengthening trust between the state and society, and actively involving the public.

This decree of the President of our country elevates cooperation between commercial banks and law enforcement agencies to a new level, within the framework of which it was determined that information on transactions of banks, payment system operators, and payment organizations will be integrated into a single electronic platform. It was also indicated that a system for informing parents about suspicious operations carried out by minors will be introduced.

In accordance with the decree, in order to improve the quality of the investigation of cybercrimes, departments for ensuring legality in the fight against cybercrimes are being created in the Prosecutor General's Office and territorial prosecutor's offices. The main task of these structures is to exercise prosecutorial supervision over the uniform application of laws in the process of investigating and solving cybercrimes.

The importance of applying a scientific approach in the effective fight against cybercrime is also not overlooked in this resolution. In particular, the Center for Combating Cybercrime and Assisting Digital Investigations, created under the Law Enforcement Academy, will be aimed at analyzing the causes and conditions that contribute to cybercrime, developing proposals for solving problems in the practice of investigation and disclosure, as

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

well as providing scientific and methodological assistance in increasing the effectiveness of investigative activities and improving the educational process.

Based on the above analysis, the need for a systematic and comprehensive approach to the effective fight against crimes committed using information technologies was once again confirmed. The sharp increase in cybercrime, the damage they cause to national security and the financial interests of citizens, require a strict policy in this direction in the country.

From this point of view, the Resolution of the President of the Republic of Uzbekistan No. PP-153 dated April 30, 2025, serves as an important regulatory framework that allows for a new approach to legal, organizational, and preventive work in this area. The decree indicates that the use of information technologies in the commission of a crime is defined as an aggravating circumstance of responsibility and punishment, as well as the following proposals are put forward to ensure cybersecurity and prevent this type of offense;

In the current Criminal Code, crimes committed through information technologies are described in various articles, scattered for each act, which creates certain difficulties in law enforcement. In this regard, the consolidation of crimes committed through information technologies in a single, separate section;

The commission of cybercrimes by bank employees and IT specialists further increases the level of danger of this crime. Because representatives of this category use all their capabilities to complete their crimes, acquire deep knowledge and skills, and adapt their activities to technological progress. Because they are well-versed in the technology of hiding from these types of crimes, they remain undetected for a long time, while simultaneously allowing them to continue committing similar crimes. Also, this category of criminals, using their special knowledge and system access capabilities, see crime (for example, information theft, money transfer) as an easy and effective tool. For example, an IT specialist can find a weakness in the system and use it for personal gain.

In this regard, to introduce into part 4 of Article 168 of the Criminal Code of the Republic of Uzbekistan the provision that the crime provided for in paragraph "g" of part 3 of this article is committed by responsible persons who have undergone training in the field of information systems, information technologies, and this circumstance is defined as an aggravating circumstance of punishment;

- Article 168 of the Criminal Code of the Republic of Uzbekistan.

Part 5 of the Criminal Code of the Republic of Uzbekistan states that in the event of compensation for material damage caused, punishment in the form of restriction of liberty and imprisonment is not applied, and if a person commits a crime of fraud through an information system, information technologies, this rule does not apply as an exception, only compensation for the damage caused is taken into account when imposing a punishment, and when imposing a punishment for crimes committed using an information system, including information and communication technologies, in addition to the main punishment, a punishment in the form of deprivation of a certain right (non-use of the Internet) is applied as an additional punishment;

- Article 3 of the Law of the Republic of Uzbekistan dated August 30, 2003 No. 530 "On Banking Secrecy" states that "Banking secrecy" consists of information on transactions, accounts, and deposits of its clients (representatives) protected by the bank, while Article 9 indicates that information constituting Banking Secrecy is transferred to the prosecutor's office, preliminary investigation and inquiry bodies with the sanction of the prosecutor based

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 05,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

on a reasoned decision of the investigator or inquiry officer in order to establish circumstances in criminal cases under their proceedings, as well as to ensure the recovery of damages or the seizure of property, and to bodies carrying out operational-search activities in order to fulfill their assigned tasks in operational-search cases under their proceedings - based on a reasoned decision approved by the head of the body carrying out operational-search activities. Therefore, it would be advisable to supplement this legal norm with a provision on the transfer of information constituting banking secrecy, with the sanction of the prosecutor, based on a reasoned decision approved by the head of the official carrying out the pre-investigation check, in order to clarify the circumstances under the documents of the pre-investigation check, conducted by officials carrying out pre-investigation checks using information technologies, as well as to ensure the recovery of the damage caused.

In conclusion, the fight against cybercrime should be carried out not only by law enforcement agencies, but also through an effective system based on the joint actions of society as a whole, highly qualified specialists, modern information technologies, and a comprehensive legislative framework.

References:

1. Ўзбекистон Республикаси Конституцияси.-Тошкент “Ўзбекистон”.-2020.

2.Ўзбекистон Республикаси Жиноят кодекси https://www.lex.uz/acts/111453

3.А.У.Анорбоев. Кибержиноятчилик, унга қарши қарши курашиш муаммолари ва киберхавфсизликни таъминлаш истиқболлари; монография, тошкент 2020 й

4. https://lex.uz/pdfs/7511360

5. https://lex.uz/docs/7511145

6. 2025 йил 5 апрел кунги “Ўзбекистон-24” телеканили орқали соат 21-00 да эфирга берилган “Ахборот” дасутуридаги Президент қарорига шарх.

7. Кибержиноятларни жиловлаш орқали хавфсиз кибермакон яратиш-А.А.Тошпўлатов “Янги Ўзбекистон” газетасини 2025 йил 7-май кунги 92-сони, 3-бети

8. https://www.pcisecuritystandards.org/document_library

9. https://www.bafin.de/SharedDocs/Downloads/EN/Aufsicht/dl_bait_en.pdf
www.chinalawtranslate.com/en/cybersecurity-law-of-the-peoples-republic-of-china/).

10. https://www.icbc-ltd.com/en/investor/annual_reports