AXBOROT SOHASIDAGI JINOYATLARNING TAVSIFI

DESCRIPTION OF CRIMES IN THE FIELD OF INFORMATION”

Ilmiy rahbar: O’zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig’i podpolkovnik

Iminov Abdurasul Abdulatipovich

O’zbekiston Respublikasi IIV Akademiyasi kunduzgi ta’lim 3-o’quv kursi 333-guruh kursanti

Rahmatullayeva Ruhshona Oybek qizi

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan cadet of group 333 of the 3rd yearofstudy

Rahmatullayeva Ruhshona Oybek qizi

A N N O T A T S I Y A

Axborot sohasidagi jinoyatlar zamonaviy raqamli jamiyat rivojlanishining muhim muammolaridan biri sifatida e’tirof etilmoqda. Axborot-kommunikatsiya texnologiyalarining jadal taraqqiy etishi, global tarmoqlarning kengayishi hamda raqamli ma’lumotlar hajmining ortib borishi ushbu turdagi jinoyatlarning ko‘payishiga zamin yaratmoqda. Axborot sohasidagi jinoyatlar deganda axborot tizimlari, kompyuter tarmoqlari va ma’lumotlar bazalariga noqonuniy kirish, ulardan ruxsatsiz foydalanish, ma’lumotlarni o‘zgartirish, yo‘q qilish yoki tarqatish bilan bog‘liq ijtimoiy xavfli qilmishlar tushuniladi.

Mazkur jinoyatlar tarkibiga noqonuniy kirish (xakerlik), zararli dasturiy vositalarni yaratish va tarqatish, shaxsga doir ma’lumotlarni noqonuniy qo‘lga kiritish, elektron to‘lov tizimlarida firibgarlik hamda axborotni qalbakilashtirish kabi harakatlar kiradi. Ushbu turdagi jinoyatlar iqtisodiy, ijtimoiy va siyosiy

sohalarga sezilarli zarar yetkazishi bilan birga, davlat va jamiyat xavfsizligiga ham tahdid soladi.

Axborot sohasidagi jinoyatlarning oldini olish kompleks yondashuvni talab etadi. Jumladan, milliy qonunchilik bazasini takomillashtirish, kiberxavfsizlikni ta'minlashning zamonaviy mexanizmlarini joriy etish, xalqaro hamkorlikni rivojlantirish hamda axborotdan foydalanish madaniyatini oshirish muhim ahamiyatga ega. Mazkur maqoladada axborot sohasidagi jinoyatlarning nazariy-huquqiy asoslari, asosiy turlari, yuzaga kelish omillari va ularni profilaktika qilish choralari ilmiy jihatdan tahlil etiladi.

Kalit so'zlar: Axborot sohasidagi jinoyatlar, kiberjinoyatchilik, axborot xavfsizligi, kompyuter tizimlari, noqonuniy kirish, zararli dasturlar, shaxsiy ma'lumotlar himoyasi, elektron firibgarlik, raqamli texnologiyalar, kiberxavfsizlik, ma'lumotlar bazasi, axborot tizimlari, huquqiy tartibga solish, profilaktika choralar.

A B S T R A C T

Crimes in the field of information are recognized as one of the key challenges in the development of modern digital society. The rapid advancement of information and communication technologies, the expansion of global networks, and the increasing volume of digital data have contributed to the growth of such crimes. Information-related crimes are defined as socially dangerous acts involving unauthorized access to information systems, computer networks, and databases, as well as the illegal use, modification, destruction, or dissemination of digital information.

These crimes include unauthorized access (hacking), the creation and distribution of malicious software, unlawful acquisition of personal data, fraud in electronic payment systems, and the falsification of digital information. Such

activities not only cause significant economic damage but also pose serious threats to social stability and national security.

The prevention of information-related crimes requires a comprehensive approach, including the improvement of national legal frameworks, the implementation of advanced cybersecurity mechanisms, the development of international cooperation, and the promotion of information literacy among users. This paper provides a scientific analysis of the theoretical and legal foundations, main types, underlying causes, and preventive measures related to crimes in the field of information.

Keywords: Information-related crimes, cybercrime, information security, computer systems, unauthorized access, malicious software, personal data protection, electronic fraud, digital technologies, cybersecurity, databases, information systems, legal regulation, preventive measures.

1. Kirish

Zamonaviy jamiyatning jadal raqamli transformatsiyasi axborot-kommunikatsiya texnologiyalarining barcha sohalarga chuqur kirib borishiga olib keldi. Bugungi kunda davlat boshqaruvi, iqtisodiyot, ta’lim, tibbiyot va ijtimoiy hayotning deyarli barcha yo‘nalishlari axborot tizimlari va raqamli platformalarga tayanmoqda. Bunday sharoitda axborotning qiymati ortib borishi bilan bir qatorda, uni noqonuniy egallash, buzish yoki o‘zgartirishga qaratilgan xavf-xatarlar ham kuchaymoqda.

Axborot sohasidagi jinoyatlar global miqyosda dolzarb muammolardan biri bo‘lib, ular kiberhududda sodir etiladigan, yuqori texnologiyalar yordamida amalga oshiriladigan ijtimoiy xavfli qilmishlar sifatida tavsiflanadi. Ushbu jinoyatlar nafaqat alohida foydalanuvchilarga, balki yirik korporatsiyalar, davlat muassasalari

va hatto milliy xavfsizlik tizimlariga ham jiddiy zarar yetkazishi mumkin. Shu boisdan axborot xavfsizligini ta'minlash va kiberjinoyatlarga qarshi samarali kurashish bugungi kunning eng muhim ilmiy-amaliy vazifalaridan biriga aylangan.

Mazkur maqolada axborot sohasidagi jinoyatlarning huquqiy va ilmiy asoslari, ularning asosiy turlari, kelib chiqish sabablari hamda ularni oldini olishga qaratilgan zamonaviy yondashuvlar tahlil qilinadi. Shuningdek, kiberxavfsizlikni mustahkamlash bo'yicha milliy va xalqaro tajribalar o'rganiladi.

1. Introduction

The rapid digital transformation of modern society has led to the deep integration of information and communication technologies into all spheres of life. Today, nearly all areas such as public administration, economy, education, healthcare, and social services rely heavily on information systems and digital platforms. In this context, while the value and significance of information continue to increase, so too do the risks associated with its illegal acquisition, manipulation, or destruction.

Information-related crimes have become one of the most pressing global challenges. These crimes are defined as socially dangerous acts committed in cyberspace through the use of advanced technologies. They may cause serious damage not only to individual users but also to large corporations, government institutions, and even national security systems. Therefore, ensuring information security and effectively combating cybercrime have become one of the most important scientific and practical tasks of the modern era.

This paper analyzes the legal and scientific foundations of information-related crimes, their main types, underlying causes, and modern approaches to their

prevention. It also examines national and international experiences in strengthening cybersecurity and developing effective protective mechanisms.

2. Axborot sohasidagi jinoyatlarning nazariy-huquqiy asoslari

Axborot sohasidagi jinoyatlar axborot xavfsizligi va kiberxavfsizlik huquqi doirasida o‘rganiladi. Ular kompyuter tizimlari, tarmoqlar va ma’lumotlarga noqonuniy kirish yoki ulardan ruxsatsiz foydalanish orqali sodir etiladigan huquqbuzarliklar hisoblanadi. Ushbu jinoyatlar milliy qonunchilik va xalqaro huquq normalari bilan tartibga solinadi.

Information crimes are studied within the framework of information security and cybersecurity law. They involve unauthorized access to computer systems, networks, or data. Such crimes are regulated by national legislation and international legal norms.

3. Axborot sohasidagi jinoyatlarning asosiy turlari

3.1 Noqonuniy kirish (xakerlik)

Xakerlik kompyuter tizimlariga ruxsatsiz kirish va ma’lumotlarni qo‘lga kiritish bilan bog‘liq jinoyat hisoblanadi.

Hacking refers to unauthorized access to computer systems and illegal acquisition of data.

3.2 Zararli dasturiy ta’minotlar

Viruslar, troyanlar va boshqa zararli dasturlar tizimlarga zarar yetkazish yoki ma’lumotlarni o‘g‘irlash uchun ishlatiladi.

Malware, including viruses and trojans, is used to damage systems or steal data.

3.3 Elektron firibgarlik

Elektron to‘lov tizimlari va internet orqali moliyaviy firibgarliklar amalga oshiriladi.

Electronic fraud is conducted through online systems and digital payment platforms.

3.4 Shaxsiy ma’lumotlarga noqonuniy egalik qilish

Shaxsiy ma’lumotlarni ruxsatsiz yig‘ish va tarqatish jiddiy huquqbuzarlik hisoblanadi.

Unauthorized collection and distribution of personal data is a serious violation.

4. Axborot sohasidagi jinoyatlarning kelib chiqish sabablari

Ushbu jinoyatlar sabablari sifatida texnologik savodsizlik, zaif xavfsizlik tizimlari, huquqiy nazoratning yetarli emasligi va moliyaviy manfaatlar ko‘rsatiladi.

The main causes include low digital literacy, weak security systems, insufficient legal control, and financial motives.

5. Axborot xavfsizligiga tahdidlar va oqibatlar

Axborot jinoyatlari iqtisodiy zarar, shaxsiy ma’lumotlarning oshkor bo‘lishi va davlat xavfsizligiga tahdid soladi.

Such crimes cause economic losses, personal data breaches, and threats to national security.

6. Axborot sohasidagi jinoyatlarning oldini olish choralari

Oldini olish uchun kiberxavfsizlikni kuchaytirish, qonunchilikni takomillashtirish, xalqaro hamkorlikni rivojlantirish va aholining axborot savodxonligini oshirish zarur.

Prevention requires strengthening cybersecurity, improving legislation, enhancing international cooperation, and increasing digital literacy.

7. Xulosa / Conclusion

Axborot sohasidagi jinoyatlar zamonaviy jamiyatning eng jiddiy muammolaridan biridir. Ularni kamaytirish uchun kompleks yondashuv, ya'ni texnik, huquqiy va ijtimoiy choralar uyg'unligi talab etiladi.

Information-related crimes are among the most serious challenges of modern society. Their reduction requires a comprehensive approach combining technical, legal, and social measures.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Stallings, W. (2018). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
2. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
3. Bishop, M. (2019). *Computer Security: Art and Science*. Addison-Wesley.
4. Kizza, J. M. (2021). *Guide to Computer Network Security*. Springer.
5. Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage Learning.
6. O'zbekiston Respublikasi Jinoyat kodeksi. Rasmiy nashr. Toshkent: Adolat, 2023.
7. O'zbekiston Respublikasi "Axborotlashtirish to'g'risida"gi Qonuni. Toshkent: Adolat, 2022.

8. O‘zbekiston Respublikasi “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. Toshkent: Adolat, 2021.

9. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. *Kiberxavfsizlik asoslari bo‘yicha o‘quv qo‘llanma*. Toshkent, 2020.

10. Karimov, A. A. (2019). *Axborot xavfsizligi va kiberhuquq asoslari*. Toshkent: O‘zbekiston Milliy universiteti nashriyoti.

LIST OF REFERENCES USED:

- Stallings, W. (2018). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
- Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
- Bishop, M. (2019). *Computer Security: Art and Science*. Addison-Wesley.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage Learning.
- Kizza, J. M. (2021). *Guide to Computer Network Security*. Springer.
- Criminal Code of the Republic of Uzbekistan. Official Edition. Tashkent: Adolat Publishing House, 2023.
- Law of the Republic of Uzbekistan “On Informatization”. Tashkent: Adolat Publishing House, 2022.
- Law of the Republic of Uzbekistan “On Personal Data”. Tashkent: Adolat Publishing House, 2021.
- Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan. *Cybersecurity Fundamentals Training Manual*. Tashkent, 2020.
- Karimov, A. A. (2019). *Fundamentals of Information Security and Cyber Law*. Tashkent: National University of Uzbekistan Press.