

# KIBERJINOYATCHILIK VA UNGA QARSHI KURASH USULLARI

## CYBERCRIME AND METHODS OF COMBATING IT

Mo'minov Haydar Muhiddinovich  
*"Realsoft Academy" MChJ direktori (Ilmiy rahbar)*

univorarsa@gmail.com

Boymamatov Akmal Akram o'g'li

*Toshkent amaliy fanlar universiteti, Axborot texnologiyalar fakulteti, KAX23-01*  
akmalboymamatov9@gmail.com

G'ayratov Mirjahon Zafarjon o'g'li

*Toshkent amaliy fanlar universiteti, Axborot texnologiyalar fakulteti, KAX23-01*  
mirjahontheend@gmail.com

Hamrayev Nuriddin Dilshod o'g'li

*Toshkent amaliy fanlar universiteti, Axborot texnologiyalar fakulteti, KAX23-01*  
hamrayevnuriddin385@gmail.com

**Annotatsiya:** Ushbu maqolada kiberjinoiyatchilik tushunchasi, uning zamonaviy raqamli jamiyatdagi o'rni va dolzarbligi tadqiq etilgan. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va internet foydalanuvchilari sonining ortishi kibertahdidlarning ko'payishiga zamin yaratmoqda. Maqolada phishing, zararli dasturlar (malware), to'lov dasturlari (ransomware) va DDoS hujumlari kabi asosiy kiberjinoiyat turlari tahlil qilingan. Shuningdek, kiberjinoiyatchilikning moliyaviy, ijtimoiy va milliy xavfsizlikka keltiruvchi salbiy oqibatlari ko'rib chiqilgan. Kiberjinoiyatlarga qarshi kurashning texnik (antivirus, shifrlash, xavfsizlik devorlari), tashkiliy (kadrlar tayyorlash, xavfsizlik siyosati) va huquqiy (qonunchilik islohatlari, xalqaro hamkorlik) usullari kompleks ravishda yoritilgan. Tadqiqot natijalari shuni ko'rsatadiki, kiberxavfsizlikni ta'minlash uchun foydalanuvchi, tashkilot va davlat darajasida muvofiqlashtirilgan yondashuv talab etiladi. Maqolaning xulosalari kiberxavfsizlik siyosatini ishlab chiquvchilar, IT mutaxassislari va keng jamoatchilik uchun amaliy ahamiyat kasb etadi.

**Kalit so'zlar:** kiberjinoiyatchilik, axborot xavfsizligi, kiberxavfsizlik, phishing, zararli dasturlar, ransomware, DDoS hujumi, ma'lu'motlarni himoya qilish, xalqaro hamkorlik, raqamli tahdid.

**Abstract:** This article investigates the concept of cybercrime, its significance, and its growing relevance in modern digital society. The rapid advancement of information and communication technologies, combined with the increasing number of internet users, has created fertile ground for the proliferation of cyber threats. The study analyzes the most prevalent types of cybercrime, including phishing, malware, ransomware, and DDoS attacks. It further examines the negative consequences of cybercriminal activity on financial systems, social trust, and national security. Technical countermeasures such as antivirus software, data encryption, and firewall systems are discussed alongside organizational strategies including staff training and security policy development, as well as legal frameworks encompassing legislative reforms and international cooperation. Findings indicate that ensuring cybersecurity requires a coordinated approach at the individual, organizational, and state levels. The article's conclusions carry practical significance for cybersecurity policymakers, IT professionals, and the general public.

**Keywords:** cybercrime, information security, cybersecurity, phishing, malware, ransomware, DDoS attack, data protection, international cooperation, digital threat.

## 1. Kirish

Hozirgi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalarini tubdan o'zgartirib yubormoqda. Internet tarmog'i, bulutli hisoblash tizimlari va mobil texnologiyalarning keng qo'llanilishi insonlar hayotini osonlashtirish bilan bir qatorda, yangi turdagi xavf va tahdidlarni ham yuzaga keltirmoqda. Xususan, kiberjinoyatchilik zamonaviy jamiyatning eng dolzarb va global muammolaridan biriga aylanib bormoqda (Anderson, 2020).

Kiberjinoyatchilik — bu axborot texnologiyalari, kompyuter tizimlari va tarmoqlar orqali amalga oshiriladigan noqonuniy harakatlar majmui bo'lib, shaxslar, tashkilotlar hamda davlatlar uchun jiddiy moliyaviy va ijtimoiy zarar keltirishi mumkin. Interpol (2022) ma'lu'motlariga ko'ra, kiberjinoyatlar global miqyosda kengayib, ularning murakkabligi va yo'naltirilganligi tobora ortib bormoqda. Bugungi kunda phishing, zararli dasturlar, to'lov dasturlari, ma'lu'motlar o'g'irlanishi va moliyaviy firibgarlik kabi kiberjinoyat turlari tobora ko'payib, ularning iqtisodiy zararini baholash qiyinlashmoqda.

Ushbu maqolaning asosiy maqsadi — kiberjinoyatchilikning mohiyatini o'rganish, uning asosiy turlari va kelib chiqish sabablarini tahlil etish hamda unga qarshi kurashning samarali texnik, tashkiliy va huquqiy usullarini yoritishdir. Tadqiqot natijalari axborot xavfsizligini ta'minlash bo'yicha ilmiy-amaliy tavsiyalar ishlab chiqishga xizmat qiladi.

## 2. Adabiyotlar sharhi va nazariy asos

Kiberjinoyatchilik va axborot xavfsizligi sohasidagi tadqiqotlar so'nggi o'n yilda sezilarli darajada kengaydi. Whitman va Mattord (2018) axborot xavfsizligining asosiy prinsiplari va tahdidlarni tasniflovchi keng qamrovli nazariy asosni ishlab chiqqan. Stallings (2017) esa kriptografiya va tarmoq xavfsizligi masalalarini chuqur o'rganib, zamonaviy himoya algoritmlarining rivojlanishini kuzatib chiqqan.

Anderson (2020) kiberxavfsizlik muhandisligi bo'yicha yozgan fundamental asarida taqsimlangan tizimlarning himoyasini ta'minlashning nazariy va amaliy jihatlarini tahlil etgan. Cisco (2023) yillik kiberxavfsizlik hisobotida phishing va ransomware hujumlarining o'tgan yillarga nisbatan 67% ga oshganligi qayd etilgan.

Jahon iqtisodiy forumi (WEF, 2024) ma'lu'motlariga ko'ra, kiberxavfsizlik global darajadagi o'nta asosiy xavf qatorida turadi. Xalqaro telekommunikatsiya ittifoqi (ITU, 2023) esa Global kiberxavfsizlik indeksida turli mamlakatlarning kiberxavfsizlik tayyorgarligi darajasini baholashda kompleks mezonlar tizimini taqdim etgan. Ushbu adabiyotlar asosida maqolada kiberjinoyatchilikning mohiyati va unga qarshi kurash usullari ko'rib chiqilgan.

## 3. Tadqiqot metodologiyasi

Ushbu tadqiqotda sifatli tahliliy metodologiya qo'llanilgan bo'lib, tadqiqot dizayni quyidagi bosqichlarni o'z ichiga olgan:

- Nazariy tahlil: Axborot xavfsizligi va kiberjinoyatchilikka oid ilmiy adabiyotlar, xalqaro tashkilotlar hisobotlari va mavjud tadqiqotlar o'rganildi. Manbalar sifatida IEEE, ACM Digital Library va Google Scholar bazalaridagi 2017–2024-yillardagi nashrlar tanlandi.
- Taqqoslash (komparativ) tahlili: Kiberjinoyatchilikka qarshi kurash bo'yicha turli mintaqalardagi yondashuvlar va xalqaro tajribalar o'zaro solishtirilib, eng samarali amaliyotlar aniqlandi.
- Tizimli tahlil: Kiberxavfsizlikni ta'minlashning texnik, tashkiliy va huquqiy jihatlarini bir-biri bilan bog'liqlikda kompleks tarzda ko'rib chiqildi.

– Umumlashtirish: Olingan ma’lu’motlar jamlanib, ilmiy xulosa va amaliy tavsiyalar shakllantirildi.

Tadqiqotda etika masalalariga alohida e’tibor qaratilgan: barcha foydalanilgan manbalar tegishli ravishda ko’rsatilgan va uchinchi shaxslar yoki tashkilotlarga oid aniq ma’lu’motlar oshkor etilmagan. Tadqiqotda insonlar ishtirokini talab etuvchi eksperimental usullar qo’llanmagan.

#### 4. Natijalar va muhokama

##### 4.1. Kiberjinoyatchilikning mohiyati va turlari

Kiberjinoyatchilik — axborot-kommunikatsiya texnologiyalari va internet tarmoqlari orqali amalga oshiriladigan noqonuniy harakatlar majmui. Kaspersky Lab (2023) tadqiqotlariga ko’ra, phishing va ransomware hujumlari so’nggi uch yilda barqaror o’sish tendentsiyasini ko’rsatmoqda. Kiberjinoyatchilarning asosiy maqsadlari qatoriga moliyaviy foyda ko’rish, maxfiy ma’lu’motlarni qo’lga kiritish va raqobatchilarga zarar yetkazish kiradi.

**1-jadval. Kiberjinoyatchilik turlari va ularning tavsifi**

| № | Kiberjinoyat turi        | Tavsifi                                              | Oqibatlari                               | Qarshi choralar                            |
|---|--------------------------|------------------------------------------------------|------------------------------------------|--------------------------------------------|
| 1 | Phishing                 | Soxta xabarlar orqali ma’lu’motlarni qo’lga kiritish | Parol va bank ma’lu’motlari o’g’irlanadi | Ehtiyotkorlik, 2FA, havolalarni tekshirish |
| 2 | Malware (zararli dastur) | Virus, troyan va boshqa zararli kodlar               | Tizim buzilishi, ma’lu’mot yo’qolishi    | Antivirus, tizimni yangilash               |
| 3 | Ransomware               | Ma’lu’motni bloklab pul talab qilish                 | Moliyaviy zarar, ma’lu’mot yo’qolishi    | Zaxira nusxa, antivirus                    |
| 4 | DDoS hujumi              | Serverga ortiqcha yuklama berish                     | Sayt va tizimlar ishlamay qoladi         | Firewall, tarmoq himoyasi                  |
| 5 | Ma’lu’mot o’g’irlash     | Shaxsiy yoki maxfiy ma’lu’motlarni qo’lga kiritish   | Maxfiylik buzilishi                      | Shifrlash, kuchli parollar                 |

##### 4.2. Kiberjinoyatchilikning kelib chiqish sabablari

Kiberjinoyatchilikning keng tarqalishiga bir qator omillar sabab bo’lmoqda. ITU (2023) ma’lu’motlariga ko’ra, raqamli muhit kengaygani sari kiberxavfsizlik tahdidlari ham mutanosib ravishda ortib bormoqda. Asosiy sabablar quyidagilardan iborat: foydalanuvchilarning axborot xavfsizligi bo’yicha bilimlarining yetarli emasligi; zaif va takrorlanuvchi parollardan foydalanish; moliyaviy manfaat va tez daromad olish istagi; kiberjinoyatlar uchun javobgarlikning yetarli darajada qat’iy emasligi; hamda texnik himoya choralarga e’tiborning kamligi (Whitman & Mattord, 2018).

##### 4.3. Kiberjinoyatchilikning oqibatlari

WEF (2024) tadqiqotiga ko'ra, kiberjinoyatchilik nafaqat individual foydalanuvchilarga, balki korporativ tizimlar va davlat infratuzilmasiga ham jiddiy zarar yetkazmoqda. Moliyaviy yo'qotishlar, reputatsion zarar, shaxsiy ma'lu'motlarning oshkor bo'lishi va tizimlar uzluksiz ishlashining buzilishi kabi oqibatlar tobora ko'proq kuzatilmoqda. Ayniqsa DDoS hujumlari davlat xizmatlarining vaqtincha to'xtab qolishiga olib kelishi aniqlangan.

#### **4.4. Kiberjinoyatchilikka qarshi kurash usullari**

Kiberjinoyatchilikka qarshi samarali kurashish uchun texnik, tashkiliy va huquqiy choralarni kompleks ravishda qo'llash zarur (Cisco, 2023):

- Texnik choralar: Antivirus dasturlari, xavfsizlik devori (firewall), IDS/IPS tizimlari, ma'lu'motlarni shifrlash, ko'p faktorli autentifikatsiya (MFA) va tizimlarni muntazam yangilash.
- Tashkiliy choralar: Xodimlar va foydalanuvchilarni axborot xavfsizligi bo'yicha o'qitish, korporativ xavfsizlik siyosatini joriy etish, tizimli monitoring va hodisalarga tezkor munosabat (Incident Response) rejalarini ishlab chiqish.
- Huquqiy choralar: Kiberjinoyatlarga qarshi qonunchilikni takomillashtirish, jinoyatchilarga nisbatan qat'iy javobgarlik choralari belgilash va xalqaro hamkorlikni kuchaytirish (UN, 2022).

#### **5. Cheklovlar**

Ushbu tadqiqotning bir qator cheklovlari mavjud. Birinchidan, tadqiqot asosan ikkilamchi manbalar (hisobotlar va ilmiy adabiyotlar) asosida amalga oshirilgan bo'lib, birlamchi empirik ma'lu'motlarni to'plash ko'zda tutilmagan. Ikkinchidan, kiberjinoyatchilik sohasidagi statistik ma'lu'motlar tez o'zgarib turishi sababli, ushbu maqoladagi ba'zi raqamlar vaqt o'tishi bilan o'z dolzarbligini yo'qotishi mumkin. Uchinchidan, turli mamlakatlarning huquqiy tizimlari va texnologik tayyorgarligi darajasidagi farqlar qiyosiy tahlilning to'liqligini cheklagan. Kelajakdagi tadqiqotlarda keng qamrovli so'rovnomalar va eksperimental usullarni qo'llash ushbu cheklovlarni bartaraf etishga yordam beradi.

#### **6. Xulosa va takliflar**

Kiberjinoyatchilik zamonaviy axborotlashgan jamiyatning eng dolzarb muammolaridan biri bo'lib, uning ko'lam va xavflilik darajasi tobora ortib bormoqda. Tahlillar shuni ko'rsatadiki, kiberjinoyatchilikning asosiy sabablari qatoriga foydalanuvchilarning axborot xavfsizligi bo'yicha yetarli bilimga ega emasligi, texnik himoya choralari ustligi va moliyaviy manfaatlar kiradi.

Kiberjinoyatchilikka qarshi samarali kurashish uchun quyidagi takliflar ishlab chiqildi:

- Davlat va xususiy sektor o'rtasida kiberxavfsizlik sohasida hamkorlikni kuchaytirish, umumiy xavf ma'lu'motlarini almashinuv platformalarini shakllantirish.
- Aholi va tashkilotlarda axborot xavfsizligi madaniyatini oshirish maqsadida muntazam treninglar va xabardorlik tadbirlarini tashkil etish.
- Zamonaviy texnologiyalar — sun'iy intellekt asosidagi kibertahdidlarni aniqlash tizimlari, blokcheyn va kvantga chidamli kriptografik algoritmlarni joriy etishga sarmoya kiritish.
- Xalqaro miqyosda kiberjinoyatlarga qarshi qonunchilikni uyg'unlashtirish va birgalikda tergov mexanizmlarini rivojlantirish.

Kelajakda kiberxavfsizlikni ta'minlashda sun'iy intellekt va innovatsion texnologiyalar muhim rol o'ynashi kutilmoqda. Shu sababli ushbu sohada ilmiy izlanishlarni kuchaytirish va amaliy choralarni takomillashtirish dolzarb vazifa bo'lib qoladi.

#### **Adabiyotlar ro'yxati**

- 
- [1] Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.
- [2] Cisco Systems. (2023). Cisco Annual Cybersecurity Report 2023. Cisco Systems Inc. <https://www.cisco.com>
- [3] International Telecommunication Union (ITU). (2023). Global Cybersecurity Index 2023. ITU Publications. <https://www.itu.int>
- [4] Interpol. (2022). INTERPOL Global Crime Trend Summary Report 2022. INTERPOL General Secretariat. <https://www.interpol.int>
- [5] Kaspersky Lab. (2023). Kaspersky Security Bulletin 2023. Kaspersky Lab. <https://www.kaspersky.com>
- [6] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.
- [7] United Nations (UN). (2022). United Nations Open-Ended Intergovernmental Expert Group on Cybercrime: Comprehensive Study on Cybercrime. UN Publications. <https://www.unodc.org>
- [8] Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.
- [9] World Economic Forum (WEF). (2024). Global Risks Report 2024. WEF Publications. <https://www.weforum.org>
- [10] O'zbekiston Respublikasining "Axborot xavfsizligi to'g'risida"gi Qonuni. (2022). O'zbekiston Respublikasi qonun hujjatlari ma'lu'otlar bazasi. <https://lex.uz>