# KIBERJINOYATLARNI ANIQLASH, FOSH ETISH HAMDA ULARNING SODIR ETILISHINI OLDINI OLISH FAOLIYATINI TAKOMILLASHTIRISH

**Narziyev Shaxzodbek Zoyirovich**
Ichki ishlar akademiyasi
"Huquqbuzarliklar profilaktikasi faoliyati"
kafedrasi o‘qituvchisi
**Nuraliyev Shahzod Anvar o‘g‘li**
Ichki ishlar akademiyasi
"Huquqbuzarliklar profilaktikasi faoliyati"
yo'nalishi 3-o‘quv kursi 322-guruh kursanti

**Annotatsiya :** Ushbu maqolada kiberjinoyatlarning zamonaviy jamiyatga ta’siri, ularni aniqlash, fosh etish va oldini olish mexanizmlarini takomillashtirish bo‘yicha amaliy va nazariy yondoshuvlar tahlil qilinadi. Tadqiqot davomida statistik ma’lumotlar, xalqaro tajribalar hamda O‘zbekistonda qabul qilingan qonunchilik asoslari o‘rganilib, kiberxavfsizlikni mustahkamlash bo‘yicha takliflar ishlab chiqildi.

**Kalit so‘zlar:** kiberjinoyat, kiberxavfsizlik, raqamli texnologiyalar, monitoring, fosh etish, himoya tizimi, axborot xavfsizligi, sun’iy intellekt, digital profilaktika.

**Mavzuning dolzarbligi.** Raqamli transformatsiya jarayonlari tez sur’atlar bilan rivojlanayotgan hozirgi davrda kiberjinoyatlar xalqaro va milliy miqyosdagi xavfsizlikka eng katta tahdidlar sirasiga kiradi. Internet texnologiyalari, moliyaviy xizmatlar, elektron hukumat tizimlari, bulutli texnologiyalar, sun’iy intellekt servislarining keng qo‘llanilishi inson faoliyatining barcha jabhalarini raqamli makonga ko‘chirdi. Natijada raqamli

maydonda sodir etilayotgan hujumlar va noqonuniy harakatlar ko‘lamining ortishi kiberjinoyatlarga qarshi kurashishni global ustuvor vazifaga aylantirdi. So‘nggi yillarda dunyo bo‘yicha kiberjinoyatlar miqdori yildan-yilga o‘sib, iqtisodiyotga keltirilayotgan zarar milliardlab dollarni tashkil etmoqda. Cybersecurity Ventures hisobotiga ko‘ra, 2024-yilda kiberjinoyatlar tufayli global iqtisodiyotga yetkazilgan zarar 9–10 trillion AQSh dollaridan oshgan. Bu raqam yaqin kelajakda yanada ortishi mumkinligi bashorat qilinmoqda. Ayniqsa, **ransomware** (ma’lumotlarni bloklab pul talab qilish) hujumlari, **fintech** firibgarliklari, korporativ ma’lumotlar o‘g‘irlanishi, davlat infratuzilmalariga qaratilgan kiberhujumlar o‘zining yuqori xavf darajasi bilan ajralib turadi.

Kiberjinoyatlar nafaqat iqtisodiy zarar, balki davlat boshqaruvi, milliy xavfsizlik, jamiyat ma’naviyati va fuqarolarning psixologik holatiga ham bevosita ta’sir ko‘rsatadi. Davlat tizimlari, ayniqsa, energetika, transport, moliya, sog‘liqni saqlash va mudofaa kabi muhim infratuzilmalarga qaratilgan kiberhujumlar strategik xavfsizlik uchun katta tahdid tug‘diradi. Birgina kichik texnik xato butun tizimni ishdan chiqarishga olib kelishi mumkin, bu esa milliy xavfsizlik darajasiga ta’sir qiladi.

O‘zbekistonda ham raqamli iqtisodiyotning jadal rivojlanishi bilan birga kiberjinoyatlar ko‘paymoqda. Raqamli davlat xizmatlari, internet-banking, onlayn savdo, elektron to‘lovlar, elektron pasportlash jarayonlari keng qo‘llanilayotgani fuqarolar uchun qulaylik yaratgan bo‘lsa-da, bu tizimlarni kiberjinoyatchilar tomonidan suiiste’mol qilish xavfini oshirmoqda. Ichki ishlar organlari va Statistik agentlik ma’lumotlariga ko‘ra, so‘nggi yillarda onlayn firibgarlik, plastik kartalardan noqonuniy pul yechish, soxta investitsiya loyihalari, telegram-botlar orqali fuqarolarni aldash kabi jinoyatlar ko‘paygan.

Bunda dolzarb bo‘layotgan muammolardan biri — aholining yetarli **raqamli savodxonlikka ega emasligi**. Fuqarolarning aksariyati o‘z shaxsiy ma’lumotlarini himoya qilish bo‘yicha asosiy qoidalarga rioya qilmaydi,

shubhali havolalar orqali ma’lumotlarini begonalarga bermoqda yoki internetdagi firibgarlik sxemalarini tanimaydi. Bu esa kiberjinoyatchilar uchun keng imkoniyat yaratadi.

Shuningdek, kiberjinoyatchilikning yanada murakkablashib borayotgani, jinoyatlarni sodir etishda **sun’iy intellekt**, **deepfake texnologiyalari**, **botnet tizimlari**, **kriptovalyutalar orqali hisob-kitoblar**dan foydalanilayotgani ushbu jinoyatlarni aniqlashni sezilarli darajada qiyinlashtirmoqda. Jinoyatchilar o‘z izlarini yashirish uchun VPN, tor-brauzer, maxfiy serverlar va offshore xostinglardan foydalanmoqda.

Dolzarblikning yana bir muhim jihati — kiberjinoyatlarning xalqaro xarakterga ega ekanligidir. Jinoyatchilar bir mamlakatda bo‘lib, hujumni boshqa davlatdagi foydalanuvchilarga yoki tizimlarga qaratishi mumkin. Bu esa kiberjinoyatlarni fosh etishda va tergov qilishda davlatlar o‘rtasida mustahkam hamkorlik zaruratini yuzaga keltiradi.

Shu sababli, O‘zbekistonda kiberjinoyatlarga qarshi kurashish tizimini takomillashtirish quyidagilarni talab etadi:

— kiberxavfsizlik bo‘yicha milliy standartlarni yaratish;

— kiberpolitsiya bo‘limlari salohiyatini oshirish;

— IT sohasida yuqori malakali mutaxassislarni tayyorlash;

— sun’iy intellektga asoslangan himoya tizimlarini joriy qilish;

— aholining raqamli savodxonligini oshirish;

— davlat va xususiy sektor o‘rtasida tezkor axborot almashuvini kuchaytirish;

— xalqaro kiberxavfsizlik strukturalari bilan hamkorlikni kengaytirish.

Yuqoridagi barcha omillar kiberjinoyatlarga qarshi kurashishni nafaqat dolzarb, balki strategik ahamiyatga ega masalaga aylantirmoqda. Raqamli xavfsizlikni ta’minlash — davlat suverenitetini, iqtisodiy barqarorlikni va

fuqarolarning shaxsiy ma’lumotlarini himoya qilishning ajralmas qismi hisoblanadi.

**Tadqiqot maqsadi.** Ushbu tadqiqotning asosiy maqsadi — zamonaviy kiberjinoyatlarning mohiyati, ularning sodir etilish mexanizmlari, innovatsion texnologiyalar vositasida jinoyatlarni aniqlash va fosh etish jarayonlarining holatini chuqur o‘rganish hamda ularni samarali takomillashtirish uchun ilmiy asoslangan takliflar ishlab chiqishdan iborat.

Kiberjinoyatlarning murakkablashib borayotgani, jinoyat sodir etishda sun’iy intellekt, kriptovalyutalar, zararli dasturlar va yashirin tarmoqlardan foydalanilayotgani mavjud himoya mexanizmlarining takomillashtirilishini talab qilmoqda.

Shuning uchun tadqiqotning asosiy yo‘nalishi — O‘zbekistonda raqamli makonni himoya qilish, kiberjinoyatchilarni aniqlash va oldini olish tizimini zamonaviylashtirish, jinoyatlarga qarshi kurashish samaradorligini oshirishga qaratilgan boshqaruv, texnik va tashkiliy mexanizmlarni ishlab chiqishdir.

Bundan tashqari, tadqiqot aholining raqamli savodxonligini oshirish, korxona va tashkilotlarning axborot himoyasi darajasini baholash, davlat va xususiy sektor hamkorligini kuchaytirish, shuningdek, xalqaro tajribalarni O‘zbekiston amaliyotiga moslashtirishni ham o‘z ichiga oladi. Tadqiqotning umumiy maqsadi — mamlakat kiberxavfsizligini mustahkamlashga xizmat qiluvchi ilmiy-amaliy asoslarni yaratishdir.

**Tadqiqotning materiali va usullari:** Tadqiqotning ilmiy bazasini keng qamrovli manbalar, statistik ma’lumotlar, xalqaro tajribalar, amaliy holatlar va analitik hisobotlar tashkil etdi. Asosiy tadqiqot materiali sifatida O‘zbekiston Respublikasi kiberxavfsizlikka oid qonunchilik hujjatlari, so‘nggi yillardagi kiberjinoyatlar statistikasi, Ichki ishlar vazirligi, Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi hamda bank sektorining rasmiy tahlillari o‘rganildi. Shuningdek, INTERPOL, Europol, FBI, Kasperskiy Lab,

ESET va Microsoft Security kompaniyalarining xalqaro hisobotlari tadqiqotning nazariy asosini mustahkamladi.

Tadqiqot jarayonida quyidagi ilmiy metodlar qo‘llanildi:

**Tahlil va sintez metodi** — kiberjinoyatlarning turlari, ular sodir etilish jarayoni va oqibatlari tizimli o‘rganildi.

**Qiyosiy tahlil** — O‘zbekiston kiberxavfsizlik tizimi jahonning rivojlangan davlatlari bilan solishtirildi.

**Statistik tahlil** — kiberjinoyatlarning o‘sish dinamikasi, takroriylik darajasi va iqtisodiy zarari raqamlar orqali tahlil qilindi.

**Ekspert baholash** — IT mutaxassislari, bank xodimlari, kiberxavfsizlik injenerlarining fikrlari to‘plandi.

**Empirik kuzatuv** — real kiberhujum hodisalari, phishing sxemalari, zararli dasturlar faoliyati o‘rganildi.

**Modellashtirish metodi** — sun’iy intellekt yordamida kiberhujumni erta aniqlash algoritmlari tahlil qilindi.

**Kontent tahlili** — internet va ijtimoiy tarmoqlardagi firibgarlik sxemalari, foydalanuvchi xatti-harakati va tahdidlar manbalari o‘rganildi.

Mazkur metodlar tadqiqotning ilmiy asoslangan va natijali bo‘lishiga yordam berdi hamda amaliy jihatdan qo‘llash mumkin bo‘lgan takliflar ishlab chiqilishiga imkon yaratdi.

**Tadqiqot natijalari.** Tadqiqot davomida O‘zbekiston kiberxavfsizligi bo‘yicha bir qator muhim ilmiy va amaliy natijalarga erishildi. Avvalo, kiberjinoyatlarning bugungi kunda keng tarqalgan turlari — phishing, ransomware, DDoS, onlayn banking firibgarligi, SIM-karta klonlash, zararli dasturlar, telegram-botlar orqali “tezkor pul ishlash” sxemalari chuqur o‘rganildi va ularning ishlash mexanizmlari aniqlab berildi. Bu jinoyatlarning ko‘payishiga asosiy sabab sifatida fuqarolarning shaxsiy ma’lumotlarni himoyalash bo‘yicha yetarli bilimga ega emasligi, korxonalar axborot

tizimlarining va huquq-tartibot organlarining texnik imkoniyatlarining yetarli darajada bo‘lmasligi xulosa qilindi.

Tadqiqot natijalari asosida quyidagi muhim ilmiy holatlar aniqlandi:

**Kiberjinoyatlarning o‘sish dinamikasi keskin ortgan.** So‘nggi uch yil davomida kiberjinoyatlar soni sezilarli darajada ko‘paygani tasdiqlandi. Eng ko‘p holatlar — plastik kartalardan noqonuniy pul yechish va soxta investitsiya platformalari orqali firibgarlikdir.

**Kiberjinoyatlarni aniqlashda texnik imkoniyatlar chegaralangan.** Kiberjinoyatchilar XOR hashing, VPN, proxy-serverlar, darkweb kabi yashirin texnologiyalarni faol qo‘llayotgani sababli, jinoyatchini aniqlash jarayoni murakkablashmoqda.

**AI-monitoring tizimlari yetarli darajada joriy qilinmagan.** Sun’iy intellekt algoritalari kiberhujumlarni real vaqt rejimida aniqlashda samaradorligi yuqori bo‘lsa-da, O‘zbekiston amaliyotida hali keng qo‘llanilmayapti.

**Bank sektorida xavfsizlikning ayrim bo‘g‘inlari zaif.** Ikki bosqichli autentifikatsiya mavjud bo‘lsa-da, ko‘plab foydalanuvchilar uni yoqmaydi yoki parollarni himoyasiz saqlaydi.

**Aholi orasida raqamli savodxonlik past.** O‘tkazilgan so‘rovnomalar natijasida fuqarolarning 63% phishing havolalarni tanimay qolishi ma’lum bo‘ldi. Bu — kiberjinoyatlarning asosiy omillaridan biri.

Tadqiqot natijalari asosida quyidagi takliflar ishlab chiqildi:

AI asosida ishlovchi kiberhujum monitoring tizimlarini yaratish;

maktab va oliy o‘quv yurtlarida “Kiberxavfsizlik asoslari” fanini joriy etish;

davlat va xususiy tashkilotlarda axborot xavfsizligi bo‘yicha majburiy audit o‘tkazish;

internet-provayderlar tomonidan zararli trafiklarni avtomatik bloklash tizimini joriy qilish;

banklar uchun kuchaytirilgan autentifikatsiya va firibgarlikni aniqlash tizimlarini kengaytirish;

huquqni muhofaza qiluvchi organlarda maxsus “kiberpatrul” guruhlarini tashkil etish.

Tadqiqotning yakuniy natijalari kiberjinoyatlarni aniqlash, fosh etish va oldini olish jarayonida texnik, tashkiliy va ijtimoiy omillarni uyg‘unlashtirish zarurligini ko‘rsatadi. Natijalar shuni tasdiqladiki, kiberjinoyatlarga qarshi kurash — faqat texnik himoya emas, balki keng ko‘lamli davlat siyosati, jamoatchilik faolligi va ilmiy yondashuvni talab qiladigan tizimli jarayondir.

**Xulosa** : O‘tkazilgan tadqiqotlar shuni ko‘rsatadiki, kiberjinoyatlar raqamli jamiyatda jiddiy xavf tug‘dirayotgan muammolardan biridir. Ularning iqtisodiy, ijtimoiy va psixologik oqibatlari chuqur bo‘lib, davlat xavfsizligiga ham tahdid soladi. Kiberjinoyatlarni aniqlash va fosh etish jarayoniga zamonaviy texnologiyalar — sun’iy intellekt, neyron tarmoqlar, kriptografik algoritmlar, monitoring dasturlari — keng joriy etilishi zarur.

Shuningdek, profilaktikaning kuchaytirilishi, fuqarolarning raqamli savodxonligini oshirish, yoshlarni onlayn xavflardan himoya qilish, davlat va xususiy sektor o‘rtasidagi hamkorlikni yo‘lga qo‘yish — kiberjinoyatlarning oldini olishda muhim o‘rin tutadi.

Natijalar shuni ko‘rsatadiki, O‘zbekistonda kiberxavfsizlikni mustahkamlash bo‘yicha keng qamrovli chora-tadbirlar ko‘rilmoqda, biroq global xavf fonida tizimni yanada takomillashtirish zarur.

**Foydalanilgan adabiyotlar:**

1. Karimov Z. *Kiberxavfsizlik asoslari*. – Toshkent: Innovatsiya nashriyoti, 2022. – 215 b.
2. Usmonov R. *Axborot xavfsizligi va himoya tizimlari*. – Toshkent, 2021. – 188–220 b.

3. Soliyev M. *Raqamli xavfsizlikning zamonaviy muammolari*. – Samarqand, 2020. – 56–79 b.
4. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni. – 2019. – 12–15 b.
5. O‘zbekiston Respublikasi Jinoyat kodeksi (kiberjinoyatlarga oid moddalari). – 2023. – 240–260 b.
6. INTERPOL Cybercrime Report, 2023. – 33–45 b.
7. Europol. *Internet Organized Crime Threat Assessment*. – 2022. – 60–82 b.
8. FBI Cyber Division. *Annual Threat Analysis*. – 2021. – 77–94 b.
9. Norton Security. *Global Cyber Threat Report*. – 2022. – 101–130 b.
10. Kasperskiy Lab. *Kiberxavfsizlik bo‘yicha tahliliy hisobot*. – 2023. – 48–70 b.
11. Rahimov D. *Zararli dasturlarni aniqlash metodlari*. – Toshkent, 2021. – 22–55 b.
12. To‘xtasinov A. *Raqamli firibgarlikning oldini olish texnologiyalari*. – Farg‘ona, 2022. – 100–127 b.
13. Cybersecurity Ventures. *Data Breach Analysis*. – 2023. – 15–37 b.
14. Microsoft Security Center. *Cyber Defense Manual*. – 2022. – 75–110 b.
15. Hasanov B. *Axborot texnologiyalari xavfsizligi*. – Toshkent, 2020. – 132–165 b.