ISSN 2181-

# “HUQUQBUZARLIKLAR PROFILAKTIKASI KUNI” DOIRASIDA FUQAROLARNING O‘ZINI-O‘ZI BOSHQARISH ORGANLARI BILAN HAMKORLIGINI 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 :** Maqolada kiberjinoyatlarning zamonaviy shakllari, ularning ijtimoiy-iqtisodiy xavfini baholash, sodir etilish mexanizmlari va ularni aniqlash, fosh etish hamda oldini olishning samarali strategiyalari tahlil qilinadi. Tadqiqotda O‘zbekistondagi amaliy holatlar, xalqaro tajribalar va zamonaviy texnologiyalar — sun’iy intellekt, big data va blokcheyn tizimlari — asosida kiberjinoyatlarni aniqlash va profilaktika mexanizmlari ko‘rib chiqildi. Maqola ilmiy-amaliy tavsiyalar bilan boyitilgan bo‘lib, davlat organlari, biznes va fuqarolar o‘rtasidagi hamkorlikni rivojlantirishga qaratilgan.

**Kalit so‘zlar:** kiberjinoyat, axborot xavfsizligi, raqamli himoya, sun’iy intellekt, profiling tizimi, ransomware, phishing, blokcheyn, onlayn firibgarlik, monitoring.

Raqamli texnologiyalar jadal rivojlanishi bilan insoniyat faoliyatining deyarli barcha sohalari internet va elektron tizimlarga ko‘chdi. Davlat boshqaruvi, moliya, ta’lim, sog‘liqni saqlash, transport va sanoat sohalari raqamli platformalarda faoliyat yuritmoqda. Shu bilan birga, internet va axborot tizimlarining kengayishi kiberjinoyatlar miqdorining oshishiga olib keldi. Kiberjinoyatlar — bu raqamli maydonda sodir etiladigan, shaxsiy, korporativ va davlat ma’lumotlarini noqonuniy o‘g‘irlash, tizimlarga zarar yetkazish yoki moliyaviy foyda

olishga qaratilgan jinoyatlar bo‘lib, ular nafaqat iqtisodiy zarar, balki milliy xavfsizlik, fuqarolarning psixologik holati va jamiyatning umumiy barqarorligiga tahdid soladi. Bugungi kunda **phishing (soxta havolalar orqali ma’lumotlarni o‘g‘irlash), ransomware (ma’lumotlarni bloklab pul talab qilish), DDoS-hujumlar (xizmatni buzish), zararli dasturlar va botnetlar orqali firibgarlik** kabi kiberjinoyatlar eng keng tarqalgan. O‘zbekiston sharoitida ham kiberjinoyatlar soni ortib bormoqda. Raqamli davlat xizmatlari, internet-banking, elektron tijorat, onlayn o‘quv platformalari va to‘lov tizimlari keng qo‘llanilishi fuqarolar va korxonalar uchun qulaylik yaratgan bo‘lsa-da, kiberjinoyatchilar uchun keng imkoniyatlar paydo bo‘lmoqda. Misol uchun, so‘nggi yillarda onlayn banking firibgarligi, plastik kartalardan noqonuniy pul yechish, soxta investitsiya platformalari va telegram-botlar orqali aldash holatlari ko‘paydi. Kiberjinoyatlarning dolzarb va xavfli bo‘lishining yana bir sababi — ularning global xarakterga ega bo‘lishidir. Jinoyatchilar bir mamlakatda bo‘lishi mumkin, ammo hujumni boshqa davlatlar foydalanuvchilariga yoki tizimlariga qaratadi. Bu esa kiberjinoyatlarni aniqlash va tergov qilishni murakkablashtiradi hamda davlatlar o‘rtasida tezkor va samarali hamkorlikni talab qiladi.Shu bilan birga, kiberjinoyatlar nafaqat texnik, balki ijtimoiy omillar orqali ham amalga oshiriladi. Fuqarolarning yetarlicha raqamli savodxon emasligi, shaxsiy ma’lumotlarni himoyalash bo‘yicha bilimlarning pastligi, firibgarlik havolalarini tanimay qolishi — kiberjinoyatlarning keng tarqalishiga asosiy omillardan biridir. Shu sababli, kiberxavfsizlikni ta’minlash uchun faqat texnik vositalar emas, balki fuqarolarni o‘qitish, xabardorlikni oshirish va xavfsizlik madaniyatini shakllantirish muhim ahamiyatga ega. Zamonaviy texnologiyalar — sun’iy intellekt, big data, blokcheyn va bulutli hisoblash tizimlari — kiberjinoyatlarni aniqlash, fosh etish va oldini olishda muhim vositalar sifatida qo‘llanilishi mumkin. Sun’iy intellekt algoritmlari kiberhujumlarni real vaqt rejimida aniqlash va tahdidlarni bashorat qilish imkonini beradi, big data tahlili esa firibgarlik faoliyatini kuzatish va aniqlashda samarali. Blokcheyn texnologiyasi esa ma’lumotlarni buzilmasligini va nazorat ostida saqlanishini kafolatlaydi. Shu sababli,

kiberjinoyatlarga qarshi kurashish tizimini takomillashtirish nafaqat texnologik, balki tashkiliy, huquqiy va ijtimoiy strategiyalarni uyg‘unlashtirishni talab qiladi. Ushbu tizim quyidagilarni o‘z ichiga olishi kerak:

- davlat va xususiy sektor o‘rtasida tezkor axborot almashuvini tashkil etish;
- IT mutaxassislari va kiberxavfsizlik ekspertlarini tayyorlash;
- sun’iy intellekt va big data asosidagi monitoring tizimlarini joriy etish;
- aholining raqamli savodxonligini oshirish bo‘yicha dasturlar ishlab chiqish;
- xalqaro kiberxavfsizlik tizimlari bilan hamkorlikni kuchaytirish.

Shunday qilib, kiberjinoyatlarni aniqlash, fosh etish va oldini olish jarayonini takomillashtirish davlat suverenitetini mustahkamlash, iqtisodiy barqarorlikni ta’minlash va shaxsiy ma’lumotlarini himoya qilishning ajralmas qismi hisoblanadi. Mazkur masala nafaqat texnologik muammo, balki milliy va xalqaro xavfsizlikni ta’minlash, jamiyatni raqamli tahdidlardan himoya qilish uchun strategik ahamiyatga ega.
Ushbu tadqiqot shuni ko‘rsatdiki, kiberjinoyatlar nafaqat iqtisodiy zarar, balki davlat boshqaruvi, milliy xavfsizlik, jamiyatning ma’naviy va psixologik barqarorligiga ham bevosita ta’sir qiladi. So‘nggi yillarda kiberhujumlar soni keskin oshganligi, ularning texnologik jihatdan murakkablashuvi va global xarakter kasb etgani — ushbu muammoning dolzarbligini yana bir bor tasdiqlaydi. Tadqiqot davomida aniqlangan asosiy natijalar quyidagilarni o‘z ichiga oladi:

1. **Kiberjinoyatlarning shakllari va mexanizmlari murakkablashmoqda.** Bugungi kunda phishing, ransomware, DDoS-hujumlar, onlayn banking firibgarligi, telegram-botlar orqali firibgarlik kabi jinoyatlar keng tarqalgan. Ularning aniqlanishi va fosh etilishi nafaqat texnik, balki ijtimoiy va huquqiy omillarga ham bog‘liq.
2. **Texnologik yechimlar yetarli darajada joriy qilinmagan.** Sun’iy intellekt, big data, blokcheyn kabi zamonaviy texnologiyalar kiberjinoyatlarni aniqlash

va oldini olishda samarali vositalardir, ammo ularning mamlakat amaliyotida keng qo‘llanilishi cheklangan.

3. **Fuqarolar va tashkilotlarning raqamli savodxonligi past.** So‘rovlar va kuzatuvlar shuni ko‘rsatdiki, ko‘plab fuqarolar shaxsiy ma’lumotlarini himoyalash bo‘yicha asosiy qoidalarga amal qilmaydi, shubhali havolalar orqali firibgarlikka uchraydi. Shu bilan birga, xususiy va davlat sektoridagi tizimlarning xavfsizlik darajasi ham barqaror emas.

4. **Davlat va xususiy sektor o‘rtasidagi hamkorlik zarurati.** Kiberjinoyatlar global xarakterga ega bo‘lgani sababli, faqat milliy darajada kurash yetarli emas. Tezkor axborot almashuv, xalqaro standartlar va tajribalarni joriy etish samarali natijaga erishishda muhim ahamiyat kasb qiladi.

5. **Profilaktika va monitoring tizimlarini takomillashtirish zarur.** Raqamli savodxonlikni oshirish, IT mutaxassislarini tayyorlash, sun’iy intellekt va big data asosidagi monitoring tizimlarini yaratish, blokcheyn texnologiyasi yordamida ma’lumotlar xavfsizligini ta’minlash kiberjinoyatlarga qarshi kurashning samarali usullaridir.

Shu bilan birga, tadqiqot shuni ko‘rsatdiki, kiberxavfsizlik faqat texnik muammo emas, balki ijtimoiy, huquqiy va strategik masala hisoblanadi. Kiberjinoyatlarni aniqlash va oldini olishning samarali tizimi — davlat suverenitetini mustahkamlash, iqtisodiy barqarorlikni ta’minlash, fuqarolarning shaxsiy ma’lumotlarini himoya qilish va jamiyatda ishonch muhitini yaratish bilan chambarchas bog‘liq. Natijada, ushbu tadqiqot asosida quyidagi ilmiy-amaliy tavsiyalar ishlab chiqildi:

- Sun’iy intellekt va big data asosidagi monitoring tizimlarini keng joriy etish;
- Fuqarolarning raqamli savodxonligini oshirish bo‘yicha davlat dasturlarini ishlab chiqish va amalga oshirish;
- Davlat va xususiy sektor o‘rtasida kiberxavfsizlik bo‘yicha tezkor axborot almashuvini tashkil etish;

• Xalqaro kiberxavfsizlik standartlari va tajribalarni mamlakat amaliyotiga moslashtirish;

• Banklar va korxonalarda kuchaytirilgan autentifikatsiya va firibgarlikni aniqlash tizimlarini joriy etish;

• Huquqni muhofaza qiluvchi organlarda maxsus “kiberpatrul” guruhlarini tashkil etish.

Shunday qilib, kiberjinoyatlarga qarshi kurashni samarali tashkil etish nafaqat texnologik innovatsiyalarni qo‘llashni, balki fuqarolarni ongli qilish, davlat boshqaruvi tizimini takomillashtirish va xalqaro hamkorlikni rivojlantirishni talab qiladi. Mazkur yondashuvlar mamlakatni global kiberxavfsizlik tahdidlaridan himoya qilishda strategik ahamiyat kasb etadi va raqamli iqtisodiyotni barqaror rivojlantirishga xizmat qiladi.

**Foydalanilgan adabiyotlar :**

1. Karimov Z. ***Kiberxavfsizlik asoslari***. Toshkent: Innovatsiya, 2023.
2. Usmonov R. ***Axborot xavfsizligi va himoya tizimlari***. Toshkent, 2022.
3. INTERPOL. ***Cybercrime Annual Report***. 2023.
4. Europol. ***Internet Organised Crime Threat Assessment (IOCTA)***. 2022.
5. Kasperskiy Lab. ***Global Cyber Threat Report***. 2023.
6. Microsoft Security. ***AI for Cybersecurity: Techniques and Tools***. 2022.
7. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida” Qonuni. 2022.
8. Norton Security. ***Cyber Threat Intelligence***. 2023.
9. Rahimov D. ***Zararli dasturlarni aniqlash va oldini olish***. Toshkent, 2021.
10. To‘xtasinov A. ***Raqamli firibgarlik va profilaktika texnologiyalari***. Farg‘ona, 2022