# 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 hozirgi zamonda keng tarqalgan ko‘rinishlari, ularning ijtimoiy va iqtisodiy xavflari, sodir etilish mexanizmlari hamda ularni aniqlash, fosh etish va oldini olishning samarali yo‘llari tahlil qilingan. Tadqiqot jarayonida O‘zbekiston amaliyoti, xalqaro tajribalar va sun’iy intellekt, big data, blokcheyn kabi ilg‘or texnologiyalarga asoslangan kiberxavfsizlik yondashuvlari o‘rganildi. Maqola davlat idoralari, biznes tuzilmalari va fuqarolar o‘rtasidagi o‘zaro hamkorlikni kuchaytirishga qaratilgan ilmiy-amaliy tavsiyalar bilan boyitilgan. **Kalit so‘zlar:** kiberjinoyat, axborot xavfsizligi, raqamli himoya, sun’iy intellekt, profiling, ransomware, phishing, blokcheyn, firibgarlik, monitoring.Raqamli texnologiyalarning keskin rivojlanishi natijasida insoniyat hayotining aksariyat jabhalari internet va elektron tizimlar bilan chambarchas bog‘lanib qoldi. Davlat boshqaruvi, moliya sektori, ta’lim, sog‘liqni saqlash, sanoat, transport va boshqa ko‘plab sohalar raqamli platformalar orqali faoliyat yuritmoqda. Shu bilan birga, internet resurslarining kengayishi kiberjinoyatlar sonining ortishiga sabab bo‘lmoqda. Kiberjinoyat — bu raqamli muhitda sodir etiladigan, shaxsiy yoki davlat axborot resurslariga noqonuniy kirish, ularni egallash, buzish yoki moliyaviy maqsadlarda foydalanishga qaratilgan noqonuniy harakatlar majmui bo‘lib, u nafaqat

iqtisodiy zarar, balki milliy xavfsizlikka tahdid, fuqarolarning ruhiy barqarorligiga ta’sir va jamiyat barqarorligiga xavf tug‘diradi. Bugungi kunda phishing, ransomware, DDoS-hujumlar, zararli dasturlar, botnetlar orqali firibgarlik kabi kiberjinoyatlar eng ko‘p uchrayotgan shakllardir.

O‘zbekiston sharoitida ham kiberjinoyatlar dinamikasi ortib bormoqda. Internet-banking, onlayn to‘lovlar, elektron tijorat va raqamli xizmatlar keng qo‘llanilishi fuqarolar uchun qulaylik yaratgani kabi, jinoyatchilar uchun ham keng imkoniyatlar ochib bermoqda. So‘nggi yillarda plastik kartalardan noqonuniy pul yechish, bank mijozlarini aldov orqali mablag‘dan mahrum qilish, soxta investitsiya platformalariga jalb qilish, telegram-botlar orqali firibgarlik kabi holatlar ko‘paygan. Kiberjinoyatlarning eng xavfli jihati — ularning xalqaro xarakterga ega bo‘lishidir. Jinoyatchi bir mamlakatda bo‘lishi mumkin, biroq hujumni butunlay boshqa hududdagi foydalanuvchilarga qaratadi. Bu esa kiberjinoyatlarni aniqlash, tekshirish va tergov qilish jarayonlarini murakkablashtiradi, davlatlar o‘rtasida kuchli hamkorlikni talab qiladi.

Kiberjinoyatlarning tarqalishiga ijtimoiy omillar ham bevosita ta’sir ko‘rsatadi. Fuqarolarning raqamli savodxonligi yetarli emasligi, shaxsiy ma’lumotlarni himoyalash bo‘yicha bilimlarning pastligi, firibgarlik sxemalarini tanimay qolish holatlari jinoyatchilar uchun qulay zamin yaratadi. Shu sababli kiberxavfsizlikni ta’minlash faqat texnik chora-tadbirlar bilan cheklanib qolmasdan, keng ko‘lamli o‘quv dasturlarini amalga oshirish, xavfsizlik madaniyatini shakllantirishni ham o‘z ichiga olishi lozim.

Zamonaviy texnologiyalar — sun’iy intellekt, big data, blokcheyn va bulutli xizmatlar — kiberjinoyatlarni aniqlash va oldini olishda muhim vosita sifatida qo‘llanilmoqda. Sun’iy intellekt real vaqt rejimida kiberhujumlarni aniqlashga yordam beradi, big data tahlili firibgarlikning yashirin sxemalarini ochib beradi, blokcheyn texnologiyasi esa ma’lumotlarning butligini kafolatlaydi.

Kiberxavfsizlik tizimini samarali shakllantirish quyidagi yondashuvlarni talab qiladi:

• davlat va xususiy sektor o‘rtasida tezkor axborot almashuvini yo‘lga qo‘yish;
• malakali IT mutaxassislarini tayyorlash;
• sun’iy intellekt va big data asosida ishlovchi monitoring tizimlarini joriy etish;
• aholi orasida raqamli savodxonlikni oshirish;
• xalqaro tajribalar bilan hamkorlikni kengaytirish.

Shunday qilib, kiberjinoyatlarni aniqlash va ularning oldini olish davlat suvereniteti, iqtisodiy barqarorlik va shaxsiy ma’lumotlarning himoyalanishi uchun strategik ahamiyat kasb etadi. Bu masala texnik yo‘nalishdan tashqari, yuridik, tashkiliy va ijtimoiy jihatlarni ham o‘z ichiga oluvchi kompleks yondashuvni talab qiladi. Tadqiqot natijalariga ko‘ra, kiberjinoyatlar nafaqat bevosita iqtisodiy yo‘qotishlarga, balki davlat boshqaruvi tizimiga, milliy xavfsizlikka va jamiyatning ma’naviy barqarorligiga ham sezilarli ta’sir ko‘rsatadi. Kiberhujumlar sonining keskin ko‘payishi, ularning murakkablashuvi va transchegaraviy xususiyati bu muammoning naqadar dolzarb ekanini yana bir bor tasdiqlaydi. Tadqiqot davomida quyidagi xulosalarga kelindi:

1. Zamonaviy kiberjinoyatlar murakkablashib bormoqda. Ularni aniqlash texnik, huquqiy va ijtimoiy omillarni o‘z ichiga oladi.
2. Sun’iy intellekt, big data va blokcheyn texnologiyalari yetarli darajada joriy qilinmagan.
3. Fuqarolar va tashkilotlar orasida raqamli savodxonlik pastligi sezilmoqda.
4. Davlat va xususiy sektor o‘rtasida kiberxavfsizlik bo‘yicha hamkorlik sust rivojlangan.
5. Monitoring va profilaktika tizimlarini modernizatsiya qilish zarur.

Tadqiqot asosida quyidagi tavsiyalar ishlab chiqildi:

• sun’iy intellekt asosidagi monitoring tizimlari joriy etilishi;
• raqamli savodxonlikni oshirish bo‘yicha davlat dasturlarini yaratish;
• davlat-xususiy sektor hamkorligini kuchaytirish;
• xalqaro kiberxavfsizlik standartlarini jalb qilish;

• bank va moliya sektorida mustahkam autentifikatsiya tizimlarini joriy etish;
• maxsus “kiberpatrul” guruhlarini tashkil etish. Kiberjinoyatlarga qarshi kurashni samarali tashkil etish mamlakatni global tahdidlardan himoyalash va raqamli iqtisodiyotning barqaror rivojlanishini ta’minlash uchun muhim omil hisoblanadi.

**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. Kaspersky Lab. ***Global Cyber Threat Report***. 2023.
6. Microsoft Security. ***AI for Cybersecurity***. 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.
11. Cisco. ***Annual Cybersecurity Report***. 2023.
12. IBM Security. ***Cost of a Data Breach***. 2023.
13. PwC. ***Global Digital Trust Insights***. 2023.
14. McAfee. ***Cybercrime Economy Analysis***. 2022.
15. MIT Technology Review. ***Future of Cyber Defense***. 2022.