ZAMONAVIY HUQUQSHUNOSLIKNING AKTUAL MUAMMOLARI

XXIII-RESPUBLIKA ILMIY-AMALIY KONFERENSIYA

YAKUNLARI BO'YICHA ILMIY ISHLAR TO'PLAMI

Issue - 4(2026) Available at www.uznauka.uz

KIBERMAKONDA SODIR ETILADIGAN O‘G‘IRLIKLARNING OLDINI OLISH MASALALARI: ILMIY-HUQUQIY TAHLIL

Olimov Dilmurod Kamol o‘g‘li – Buxoro shahar IIO FMB 1-son IIB JQB tezkor vakili katta leytenant

Annotatsiya. *Mazkur tezisda kibermakonda sodir etiladigan o‘g‘irlik jinoyatlarining mohiyati, ularning sodir etilish usullari hamda ularni oldini olishning huquqiy, tashkiliy va texnik mexanizmlari tahlil qilinadi. Shuningdek, zamonaviy axborot texnologiyalarining rivojlanishi sharoitida kiberjinoyatchilikka qarshi kurashishning dolzarb yo‘nalishlari, xalqaro tajriba va milliy amaliyot asosida taklif va tavsiyalar ishlab chiqilgan.*

Kalit so‘zlar: *kibermakon, kiberjinoyat, o‘g‘irlik, phishing, malware, axborot xavfsizligi, profilaktika, raqamli himoya.*

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi zamonaviy jamiyatning barcha ijtimoiy-iqtisodiy, siyosiy va huquqiy munosabatlarini tubdan o‘zgartirib, ularni raqamli shaklga o‘tkazdi. Raqamlashtirish jarayoni davlat boshqaruvi, bank-moliya tizimi, savdo, ta’lim, sog‘liqni saqlash va boshqa ko‘plab sohalarda samaradorlikni oshirish, tezkorlik va shaffoflikni ta’minlashga xizmat qilmoqda. Shu bilan birga, mazkur jarayon yangi turdagi xavf va tahdidlarni, xususan, kibermakonda sodir etiladigan huquqbuzarliklarning keskin ortishini yuzaga keltirmoqda.

Kibermakonda sodir etiladigan o‘g‘irlik jinoyatlari an’anaviy o‘g‘irlikdan o‘zining usullari, vositalari va obyekti bilan tubdan farq qiladi. Agar ilgari o‘g‘irlik moddiy boyliklarni bevosita egallash orqali amalga oshirilgan bo‘lsa, hozirgi davrda u axborot resurslariga noqonuniy kirish, shaxsiy va moliyaviy ma’lumotlarni qo‘lga kiritish hamda ulardan foydalanish orqali sodir etilmoqda. Xususan, bank kartalari rekvizitlarini firibgarlik yo‘li bilan egallash (phishing), zararli dasturlar (malware) orqali foydalanuvchi qurilmalariga kirib borish, elektron hamyon va onlayn to‘lov tizimlarini buzish, shuningdek, identifikatsiya ma’lumotlarini o‘g‘irlash kabi holatlar keng tarqalgan.

Bundan tashqari, kibermakondagi o‘g‘irlik jinoyatlarining yana bir muhim xususiyati – ularning yuqori darajada yashirinlikka ega bo‘lishi va transmilliy xarakter kasb etishidir. Jinoyatchilar zamonaviy texnologiyalardan, jumladan, anonimlashtirish vositalari (VPN, TOR tarmoqlari), kriptovalyutalar hamda murakkab texnik usullardan foydalangan holda o‘z izlarini yashirishga harakat qiladilar. Bu esa bunday jinoyatlarni aniqlash, fosh etish va tergov qilish jarayonini sezilarli darajada murakkablashtiradi.

Mazkur sharoitda kiberxavfsizlikni ta’minlash masalasi nafaqat texnik, balki kompleks huquqiy, tashkiliy va institutsional yondashuvni talab etadi. Avvalo, milliy qonunchilikni zamon talablariga mos ravishda takomillashtirish, xususan, shaxsga doir ma’lumotlarni himoya qilish, elektron dalillarning maqbulligini ta’minlash va kiberjinoyatlar uchun javobgarlik choralarini kuchaytirish muhim ahamiyat kasb etadi. Shu bilan birga, huquqni muhofaza qiluvchi organlarning

texnik imkoniyatlarini kengaytirish, raqamli kriminalistika sohasida malakali kadrlar tayyorlash ham dolzarb vazifalardan biridir.

Profilaktika choralariga alohida e’tibor qaratish zarur. Bu borada aholi o‘rtasida kiberxavfsizlik madaniyatini shakllantirish, foydalanuvchilarning axborot xavfsizligi bo‘yicha savodxonligini oshirish, shuningdek, davlat va xususiy sektor o‘rtasida samarali hamkorlikni yo‘lga qo‘yish muhim hisoblanadi. Texnik jihatdan esa zamonaviy himoya vositalari – kriptografik tizimlar, ko‘p bosqichli autentifikatsiya, sun’iy intellekt asosidagi monitoring va aniqlash tizimlarini joriy etish orqali kiberxavfsizlik darajasini oshirish mumkin.

Xulosa qilib aytganda, axborot-kommunikatsiya texnologiyalarining rivojlanishi bilan bog‘liq holda yuzaga kelayotgan kibermakondagi o‘g‘irlik jinoyatlari jamiyat uchun jiddiy xavf tug‘diradi. Ularning oldini olish va samarali kurashish faqatgina kompleks yondashuv – huquqiy tartibga solish, texnik himoya, institutsional rivojlanish va profilaktik chora-tadbirlarning uyg‘unligi orqali ta’minlanishi mumkin.

Kibermakonda sodir etiladigan o‘g‘irlik bu axborot-kommunikatsiya texnologiyalari, kompyuter tizimlari va telekommunikatsiya tarmoqlaridan foydalangan holda boshqa shaxsga tegishli mol-mulkni, pul mablag‘larini yoki raqamli aktivlarni noqonuniy ravishda egallashga qaratilgan ijtimoiy xavfli qilmish sifatida namoyon bo‘ladi. Mazkur jinoyat turi an’anaviy o‘g‘irlikdan farqli ravishda moddiy predmetlarni bevosita olib qo‘yish emas, balki axborotga noqonuniy kirish, uni manipulyatsiya qilish yoki undan foydalanish orqali amalga oshiriladi.

Ilmiy nuqtai nazardan, kibermakondagi o‘g‘irlik jinoyatlari axborot xavfsizligining uch asosiy komponenti — maxfiylik (confidentiality), yaxlitlik (integrity) va mavjudlik (availability) tamoyillarining buzilishi bilan chambarchas bog‘liqdir. Ayniqsa, maxfiy ma’lumotlarning (bank rekvizitlari, login-parollar, biometrik identifikatorlar) noqonuniy qo‘lga kiritilishi ushbu jinoyatlarning asosiy mexanizmini tashkil etadi.

Kibermakonda jinoyatchilar o‘z shaxsini yashirish uchun turli texnologik vositalardan — VPN, TOR tarmoqlari, proksi-serverlar va kriptovalyutalardan foydalanadilar. Bu holat jinoyat subyektini aniqlashni murakkablashtirib, huquqni muhofaza qiluvchi organlar faoliyatida sezilarli qiyinchiliklar tug‘diradi. Natijada javobgarlikdan qochish ehtimoli ortadi.

Mazkur jinoyatlar geografik chegaralardan mustaqil ravishda sodir etilishi bilan ajralib turadi. Jinoyatchi bir davlat hududida bo‘lib, boshqa davlatdagi shaxs yoki tashkilotga nisbatan jinoyat sodir etishi mumkin. Bu esa xalqaro huquqiy hamkorlik, ekstraditsiya, yurisdiksiya va dalillar almashinuvi kabi masalalarni dolzarb qiladi.

Raqamli texnologiyalar orqali qisqa vaqt ichida katta miqdordagi moliyaviy resurslarni o‘zlashtirish imkoniyati mavjud. Masalan, bank tizimlariga noqonuniy kirish yoki to‘lov tizimlarini buzish orqali bir necha soniya ichida millionlab mablag‘lar o‘tkazilishi mumkin. Bu esa jinoyatning ijtimoiy xavflilik darajasini yanada oshiradi.

Kibermakondagi o‘g‘irlik jinoyatlari yuqori darajadagi texnik bilim, dasturlash ko‘nikmalari, axborot tizimlarining zaifliklarini aniqlash va ulardan foydalanish qobiliyatini talab etadi. Ko‘pincha bunday jinoyatlar zararli dasturlar (malware), fishing (phishing), ijtimoiy muhandislik usullari yoki eksploitlar yordamida amalga oshiriladi.

An’anaviy o‘g‘irlikdan farqli o‘laroq, bu turdagi jinoyatlarda moddiy emas, balki nomoddiy aktivlar — elektron pullar, kriptovalyutalar, ma’lumotlar bazalari, intellektual mulk obyektlari nishon bo‘ladi. Shu bois ularni aniqlash va baholashda o‘ziga xos yondashuv talab etiladi.

Kibermakondagi o‘g‘irliklar ko‘pincha uzoq vaqt davomida sezilmasdan sodir etiladi. Jabrlanuvchi o‘z mablag‘larining o‘g‘irlanganini darhol emas, balki ma’lum vaqt o‘tgach aniqlashi mumkin. Bu esa jinoyatni fosh etish jarayonini murakkablashtiradi.

Kibermakonda sodir etiladigan o‘g‘irlik jinoyatlari turli texnologik va psixologik usullar orqali amalga oshiriladi. Ushbu usullar zamonaviy axborot tizimlarining zaifliklari hamda inson omilidan kompleks tarzda foydalanishga asoslanadi. Amaliyotda eng ko‘p uchraydigan kibero‘g‘irlik usullarini quyidagicha ilmiy asosda tahlil qilish mumkin.

1. Phishing bu foydalanuvchini aldash orqali uning maxfiy ma’lumotlarini (login, parol, bank karta rekvizitlari, SMS-kodlar va boshqalar) qo‘lga kiritishga qaratilgan kiberjinoyat usulidir. Ushbu usul odatda ishonchli tashkilotlar (banklar,

davlat organlari, mashhur servislar) nomidan yuborilgan soxta elektron xatlar, SMS-xabarlar yoki veb-sahifalar orqali amalga oshiriladi.

Ilmiy jihatdan phishing ijtimoiy muhandislikning eng keng tarqalgan ko‘rinishi bo‘lib, u inson psixologiyasiga — ishonuvchanlik, qo‘rquv, shoshilinch qaror qabul qilish kabi omillarga ta’sir qilish orqali muvaffaqiyatga erishadi. Zamonaviy shakllari (spear-phishing, whaling) aniq shaxs yoki tashkilotga yo‘naltirilganligi bilan ajralib turadi.

2.Malware bu foydalanuvchi qurilmasiga yashirin tarzda o‘rnatilib, ma’lumotlarni o‘g‘irlash, tizim faoliyatini buzish yoki jinoyatchiga masofadan nazorat qilish imkonini beruvchi zararli dasturiy ta’minotdir. Ular viruslar, trojanlar, spyware, ransomware kabi turlarga bo‘linadi.

Mazkur usul orqali jinoyatchilar klaviatura orqali kiritilgan ma’lumotlarni qayd etish (keylogging), fayllarni nusxalash, bank ilovalariga kirish yoki foydalanuvchi nomidan operatsiyalarni amalga oshirish imkoniyatiga ega bo‘ladi. Ilmiy nuqtai nazardan, malware axborot tizimlarining texnik zaifliklaridan foydalanishga asoslangan bo‘lib, ko‘pincha dasturiy ta’minotdagi xatoliklar (vulnerabilities) orqali tarqaladi.

3.Hacking bu kompyuter tizimlari, serverlar yoki tarmoqlarga ruxsatsiz kirish orqali ulardagi ma’lumotlarni o‘zgartirish, yo‘q qilish yoki o‘g‘irlashga qaratilgan faoliyatdir. Kibero‘g‘irlik kontekstida hacking asosan moliyaviy ma’lumotlar, mijozlar bazasi yoki to‘lov tizimlariga noqonuniy kirish bilan bog‘liq.

Ushbu usulda jinoyatchilar zaif parollar, autentifikatsiya tizimidagi kamchiliklar yoki dasturiy xatoliklardan foydalanadilar. Ilmiy jihatdan hacking yuqori darajadagi texnik bilim va analitik fikrlashni talab etadi hamda ko‘pincha oldindan rejalashtirilgan va tizimli tarzda amalga oshiriladi.

4. Ijtimoiy muhandislik bu texnik vositalardan ko‘ra ko‘proq inson psixologiyasiga ta’sir ko‘rsatish orqali maxfiy ma’lumotlarni qo‘lga kiritish usulidir. Jinoyatchi o‘zini bank xodimi, texnik yordam mutaxassisi yoki davlat organi vakili sifatida tanishtirib, foydalanuvchini aldash orqali kerakli ma’lumotlarni olishga erishadi.

Mazkur usulning asosiy ustunligi shundaki, u texnik himoya vositalarini chetlab o‘tadi, chunki ma’lumotni bevosita foydalanuvchining o‘zi taqdim etadi. Ilmiy jihatdan bu usul kriminologiyada “inson zaifligi omili” sifatida baholanadi va kibero‘g‘irliklarning muhim qismi aynan shu omil bilan bog‘liq.

Kibermakonda sodir etiladigan o‘g‘irlik jinoyatlariga qarshi kurashishda huquqiy mexanizmlar markaziy o‘rin egallaydi. Zamonaviy raqamli muhitda jinoyatlar tezkorlik, anonimlik va transmilliylik xususiyatlariga ega bo‘lgani sababli, ularni samarali oldini olish faqatgina mukammal normativ-huquqiy baza va uni amaliyotda to‘g‘ri qo‘llash orqali ta’minlanadi. Shu nuqtai nazardan, quyidagi yo‘nalishlar alohida ilmiy ahamiyat kasb etadi:

a) kibermakonda o‘g‘irliklarning oldini olishda, avvalo, milliy qonunchilikni zamonaviy tahdidlarga moslashtirish zarur. Bu borada axborot xavfsizligi, shaxsga doir ma’lumotlarni himoya qilish, elektron tijorat va raqamli xizmatlar sohasini tartibga soluvchi qonunlar muhim o‘rin tutadi. Xususan, “Axborotlashtirish

to‘g‘risida”, “Shaxsga doir ma’lumotlar to‘g‘risida”, “Elektron hukumat to‘g‘risida” kabi normativ hujjatlar kibermakon munosabatlarini huquqiy jihatdan tartibga solishda asosiy manba hisoblanadi. Ilmiy jihatdan qaraganda, ushbu qonunlar nafaqat jinoyat sodir etilgandan keyingi javobgarlikni belgilashi, balki profilaktik (oldini oluvchi) xarakterga ega bo‘lishi, ya’ni xavf omillarini kamaytirishga qaratilgan normalarni ham o‘z ichiga olishi lozim;

b) kibermakondagi jinoyatlarni tergov qilishda elektron dalillar hal qiluvchi ahamiyatga ega. Elektron dalillar bu raqamli shaklda saqlanadigan va jinoyat holatini isbotlashga xizmat qiluvchi axborot (log-fayllar, IP-manzillar, elektron yozishmalar, server ma’lumotlari va boshqalar)dir. Mazkur yo‘nalishda asosiy muammo elektron dalillarning ishonchliligi, yaxlitligi va qonuniy yo‘l bilan olinganligini ta’minlashdir. Shu sababli, protsessual qonunchilikda elektron dalillarni yig‘ish, saqlash, ekspertizadan o‘tkazish va sudda baholash tartibini aniq belgilash zarur. Ilmiy yondashuvda bu jarayon “raqamli kriminalistika” tamoyillari asosida amalga oshirilishi lozim, ya’ni dalilga zarar yetkazmaslik, uning asl holatini saqlash va izchil hujjatlashtirish talab etiladi;

c) kibermakondagi o‘g‘irlik jinoyatlarining ko‘pchiligi transmilliy xarakterga ega bo‘lib, bir necha davlat hududida sodir etilishi yoki turli yurisdiksiyalar bilan bog‘liq bo‘lishi mumkin. Shu bois bunday jinoyatlarga qarshi kurashishda xalqaro hamkorlik muhim ahamiyat kasb etadi. Bu borada davlatlar o‘rtasida axborot almashinuvi, jinoyatchilarni ekstraditsiya qilish, qo‘shma tergov harakatlarini o‘tkazish va xalqaro konvensiyalar doirasida hamkorlik qilish zarur. Xususan, kiberjinoyatchilikka qarshi xalqaro standartlarni belgilovchi hujjatlar

(masalan, Budapesht konvensiyasi) ushbu sohada yagona yondashuvni shakllantirishga xizmat qiladi;

d) kibermakonda sodir etiladigan o‘g‘irlik jinoyatlariga nisbatan jinoiy javobgarlik choralarini takomillashtirish ham dolzarb masalalardan biridir. Amaldagi qonunchilikda bunday jinoyatlar uchun sanksiyalar belgilangan bo‘lsa-da, ularni zamonaviy tahdidlar darajasiga moslashtirish zarur. Ilmiy nuqtai nazardan, javobgarlik choralarini belgilashda quyidagi omillar inobatga olinishi lozim:

- jinoyatning ijtimoiy xavflilik darajasi;
- yetkazilgan zarar miqdori;
- jinoyatning uyushgan guruh tomonidan sodir etilganligi;
- axborot tizimlariga yetkazilgan zarar oqibatlari.

Shuningdek, muqobil javobgarlik choralarini (jarima, axborot tizimlaridan foydalanish huquqini cheklash, majburiy ta’lim dasturlari) qo‘llash imkoniyatlarini ham kengaytirish maqsadga muvofiq.

Kibermakonda sodir etiladigan o‘g‘irlik jinoyatlarining oldini olishda faqat huquqiy mexanizmlar yetarli bo‘lmay, balki ularni samarali qo‘llab-quvvatlovchi tashkiliy va texnik profilaktika choralarini kompleks tarzda amalga oshirish zarur. Zamonaviy kiberxavfsizlik konsepsiyasida “ko‘p darajali himoya” (multi-layered security) yondashuvi ustuvor hisoblanib, unda inson omili, tashkiliy boshqaruv va texnologik vositalar o‘zaro uyg‘un holda ishlashi talab etiladi.

Kibermakonda sodir etiladigan o‘g‘irliklarning oldini olishda tashkiliy va texnik profilaktika choralarining o‘rni alohida ahamiyat kasb etadi. Zamonaviy

axborot jamiyatida kiberxavfsizlikni ta’minlash faqat texnik vositalar bilan cheklanib qolmay, balki institutsional tizimlar, boshqaruv mexanizmlari hamda inson omilini o‘z ichiga olgan kompleks yondashuvni talab etadi. Shu bois mazkur yo‘nalishda tashkiliy va texnik choralar o‘zaro uyg‘un holda amalga oshirilishi lozim.

Avvalo, davlat organlari va xususiy sektor o‘rtasidagi hamkorlikni kuchaytirish muhim strategik vazifa hisoblanadi. Chunki zamonaviy axborot infratuzilmasining asosiy qismi, xususan bank tizimlari, telekommunikatsiya tarmoqlari va elektron tijorat platformalari xususiy sektor tasarrufida faoliyat yuritadi. Shu sababli kiberxavfsizlikni ta’minlashda yagona markazlashgan yondashuvni shakllantirish uchun davlat va biznes subyektlari o‘rtasida samarali hamkorlik mexanizmlarini yo‘lga qo‘yish zarur. Bu, o‘z navbatida, kiberinsidentlar haqida tezkor axborot almashinuvi, qo‘shma xavfsizlik standartlarini ishlab chiqish hamda kiberhujumlarga nisbatan muvofiqlashtirilgan tezkor javob choralarini ko‘rishni taqozo etadi. Ilmiy jihatdan ushbu jarayon “public-private partnership” modeli asosida amalga oshirilib, milliy kiberxavfsizlik tizimining barqarorligini ta’minlashga xizmat qiladi.

Shu bilan birga, kiberxavfsizlik sohasida maxsus bo‘linmalar faoliyatini rivojlantirish ham muhim tashkiliy choralar sirasiga kiradi. Xususan, CERT/CSIRT markazlari, kiberpolitsiya tuzilmalari va raqamli kriminalistika laboratoriyalari kibermakondagi tahdidlarni aniqlash va ularga qarshi kurashishda asosiy institutsional subyektlar hisoblanadi. Ushbu bo‘linmalar kiberinsidentlarni aniqlash, ularni tahlil qilish, tahdidlar monitoringini yuritish, tezkor choralar

ko‘rish hamda profilaktik tavsiyalar ishlab chiqish kabi funksiyalarni bajaradi. Ularning samarali faoliyati zamonaviy texnik vositalar bilan ta’minlanganlik darajasi hamda yuqori malakali kadrlar salohiyatiga bevosita bog‘liqdir.

Kibero‘g‘irliklarning oldini olishda inson omili alohida ahamiyatga ega bo‘lganligi sababli, aholi o‘rtasida raqamli savodxonlikni oshirish zarurati ham dolzarb hisoblanadi. Amaliyot shuni ko‘rsatadiki, kiberjinoyatlarning aksariyati foydalanuvchilarning yetarli bilimga ega emasligi, ehtiyotsizligi yoki ijtimoiy muhandislik usullariga aldanishi natijasida sodir etiladi. Shu bois aholiga phishing hujumlari, zararli dasturlar va boshqa tahdidlardan himoyalanish bo‘yicha tushuntirish ishlari olib borish, ommaviy axborot vositalari orqali targ‘ibot qilish hamda ta’lim tizimida kiberxavfsizlikka oid bilimlarni joriy etish muhim profilaktik vosita hisoblanadi. Ilmiy yondashuvda bu yo‘nalish viktimologik profilaktika sifatida e’tirof etilib, potentsial jabrlanuvchilarning xabardorligini oshirish orqali jinoyatlarning oldini olishga qaratilgan.

Texnik choralar esa axborot tizimlarini bevosita himoya qilishga qaratilgan bo‘lib, ular kibero‘g‘irliklarga qarshi kurashishda amaliy jihatdan eng muhim vositalardan hisoblanadi. Jumladan, antivirus dasturlari zararli dasturlarni aniqlash va yo‘q qilishga xizmat qilsa, firewall tizimlari tarmoq trafigini nazorat qilish orqali ruxsatsiz kirishlarning oldini oladi. Ushbu vositalar axborot tizimlarining birlamchi himoya darajasini tashkil etadi.

Bundan tashqari, ma’lumotlarni shifrlash texnologiyalari axborot xavfsizligini ta’minlashda muhim o‘rin tutadi. Shifrlash orqali ma’lumotlar maxsus algoritmlar asosida kodlanadi va ruxsatsiz shaxslar uchun tushunarsiz holga

keltiriladi. Bu usul ayniqsa bank operatsiyalari, elektron tijorat va davlat axborot tizimlarida keng qo‘llanilib, axborotning maxfiyligini ta’minlaydi.

Ikki bosqichli autentifikatsiya (2FA) tizimlari esa foydalanuvchi identifikatsiyasini yanada ishonchli qiladi. Parolga qo‘shimcha ravishda bir martalik kod, biometrik ma’lumot yoki maxsus token orqali tasdiqlash talab etilishi hisoblarni noqonuniy egallash ehtimolini keskin kamaytiradi. Bu usul zamonaviy kiberxavfsizlik amaliyotida keng qo‘llanilayotgan samarali himoya mexanizmlaridan biridir.

Shuningdek, tarmoq monitoringi va tahdidlarni aniqlash tizimlari ham alohida ahamiyatga ega. IDS/IPS va SIEM kabi tizimlar real vaqt rejimida axborot oqimlarini tahlil qilib, shubhali faoliyatni aniqlash, kiberhujumlarni oldindan prognoz qilish va tezkor choralar ko‘rish imkonini beradi. Zamonaviy ilmiy yondashuvda bunday tizimlar sun’iy intellekt va katta ma’lumotlar texnologiyalari bilan integratsiyalashgan holda ishlaydi, bu esa ularning samaradorligini yanada oshiradi.

Kibermakonda sodir etiladigan o‘g‘irliklar zamonaviy axborot jamiyatining eng dolzarb muammolaridan biri bo‘lib, ularning oldini olish kompleks, tizimli va uzviy yondashuvni talab etadi. Tadqiqot natijalari shuni ko‘rsatadiki, kibero‘g‘irliklar nafaqat texnologik zaifliklar, balki huquqiy bo‘shliqlar, foydalanuvchilarning past darajadagi kiberxavfsizlik madaniyati hamda davlat va xususiy sektor o‘rtasidagi hamkorlikning yetarli emasligi bilan ham chambarchas bog‘liq.

Ilmiy-huquqiy tahlil asosida quyidagi xulosalarga kelish mumkin: birinchidan, kiberjinoyatlarning oldini olishda normativ-huquqiy bazani takomillashtirish, xususan, raqamli dalillar, shaxsga doir ma’lumotlarni himoya qilish va transmilliy jinoyatlarga qarshi kurashish mexanizmlarini kuchaytirish muhim ahamiyat kasb etadi. Ikkinchidan, zamonaviy texnologiyalar, jumladan sun’iy intellekt, big data va real vaqt monitoring tizimlarini joriy etish orqali kiberxavflarni erta aniqlash va bartaraf etish imkoniyati kengayadi. Uchinchidan, davlat organlari, xususiy sektor va fuqarolar o‘rtasida samarali hamkorlikni yo‘lga qo‘yish kibero‘g‘irliklarga qarshi kurashda muhim omil hisoblanadi.

Shuningdek, profilaktika choralarini kuchaytirish, aholining raqamli savodxonligini oshirish, maxsus malakali kadrlarni tayyorlash hamda xalqaro tajribani milliy amaliyotga moslashtirish orqali kibermakondagi o‘g‘irliklarning oldini olish samaradorligini oshirish mumkin.

Umuman olganda, kibero‘g‘irliklarga qarshi kurash faqatgina huquqni muhofaza qiluvchi organlar zimmasidagi vazifa bo‘lib qolmay, balki jamiyatning barcha qatlamlari ishtirokini talab etadigan keng qamrovli va uzluksiz jarayon sifatida qaralishi lozim.

TAVSIYA ETILADIGAN ADABIYOTLAR

1.Abdullayev, A. – *Kiberxavfsizlik asoslari*. Toshkent: Fan va texnologiya, 2021.

2.Ergashev, B. – *Axborot xavfsizligi va huquqiy tartibga solish*. Toshkent: TDYU nashriyoti, 2020.

3.Karimov, Sh. – *Raqamli iqtisodiyot va kiberxavfsizlik muammolari*. Toshkent: Iqtisodiyot, 2022.

4.Raxmonov, D. – *Kiberjinoyatchilikka qarshi kurashning huquqiy asoslari*. Toshkent: Adolat, 2019.

5.Yuldashev, O. – *Axborot texnologiyalari va huquq*. Toshkent: Yangi asr avlodi, 2021.

6.Brenner, S. W. – *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston: Northeastern University Press, 2010.

7.Clough, J. – *Principles of Cybercrime*. Cambridge: Cambridge University Press, 2015.

8.Goodman, M. – *Future Crimes: Everything Is Connected, Everyone Is Vulnerable*. New York: Anchor Books, 2016.

9.Wall, D. S. – *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2007.

10.Yar, M. – *Cybercrime and Society*. London: Sage Publications, 2018.