KIBERJINOYATCHILIKNING OLDINI OLISHDA TEZKOR-QIDIRUV TADBIRLARINI HUQUQIY TARTIBGA SOLISH: KRIMINOLOGIK TAHLIL

BOBOMURODOV
Farxod Boymurotovich
Toshkent xalqaro universiteti Yurisprudensiya fakulteti
Huquqiy fanlar kafedrasi dotsent v.b.,
yuridik fanlar doktori (DSc)

Annotatsiya. *Mazkur maqolada kiberjinoyatchilikning oldini olishda tezkor-qidiruv tadbirlarini huquqiy tartibga solishning kriminologik va huquqiy jihatlari tahlil qilingan. Kiberjinoyatchilikning sabablari va shart-sharoitlari, jinoyatchining shaxsi, viktimologik omillar, raqamli muhitdagi kriminogen vaziyat hamda profilaktika mexanizmlari kriminologiya nuqtayi nazaridan yoritilgan.*
Kalit so‘zlar: kiberjinoyatchilik, kriminologiya, tezkor-qidiruv faoliyati, kiberprofilaktika, elektron dalillar, raqamli kuzatuv, viktimologiya, kiberdeviasiya, kriminogen omillar, kiberxavfsizlik, sun’iy intellekt.

Аннотация. *В данной статье проанализированы криминологические и правовые аспекты правового регулирования оперативно-розыскных мероприятий, направленных на профилактику киберпреступности. С криминологической точки зрения освещены причины и условия киберпреступности, личность преступника, виктимологические факторы, криминогенная ситуатсия в цифровой среде, а также механизмы профилактики.*
Ключевые слова: *киберпреступность, криминология, оперативно-розыскная деятельность, киберпрофилактика, электронные доказательства, цифровое наблюдение, виктимология, кибердевиация, криминогенные факторы, кибербезопасность, искусственный интеллект.*

Abstract. *This scientific article analyzes the criminological and legal aspects of regulating operational-search measures aimed at preventing cybercrime. From a criminological perspective, the article examines the causes and conditions of cybercrime, the personality of offenders, victimological factors, the criminogenic situation within the digital environment, and mechanisms of cybercrime prevention.*
Keywords: *cybercrime, criminology, operational-search activity, cyber prevention, electronic evidence, digital surveillance, victimology, cyber deviation, criminogenic factors, cybersecurity, artificial intelligence.*

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi, davlat va jamiyat hayotining raqamlashuvi [5], elektron davlat xizmatlari, onlayn bank tizimlari, elektron tijorat va sun’iy intellekt texnologiyalarining keng joriy etilishi kibermakonda yangi turdagi jinoyatlarning ko‘payishiga olib kelmoqda. Xususan, kiberjinoyatchilik transmilliy, yuqori latentlikka ega hamda tez o‘zgaruvchan jinoyat turi sifatida jahon xavfsizligiga jiddiy tahdid solmoqda.

Xalqaro tahlillarga ko‘ra, 2025-yilga kelib global kiberjinoyatlar natijasida yetkaziladigan iqtisodiy zarar hajmi yillik 10,5 trillion AQSH dollariga yetishi prognoz qilingan. Bu esa kiberjinoyatchilikni jahon iqtisodiyoti uchun xavfli transmilliy tahdidlardan biriga aylantirmoqda. Ayniqsa, fishing, shaxsga doir ma’lumotlarni o‘g‘irlash, internet-banking orqali firibgarlik, kriptovalyuta bilan bog‘liq jinoyatlar hamda davlat axborot tizimlariga qilingan hujumlar soni yil sayin ortib bormoqda.

Jahon amaliyotida Interpol, Europol hamda Federal Bureau of Investigation ma’lumotlariga ko‘ra, kiberjinoyatchilikning aksariyati Internet tarmog‘i orqali masofadan turib amalga oshirilishi, jinoyatchilarning anonimlik imkoniyati yuqoriligi va elektron dalillarni tez yo‘q qilish imkoniyati mavjudligi sababli ushbu jinoyatlarni aniqlash va fosh etish an’anaviy jinoyatlarga nisbatan ancha murakkab hisoblanadi. Shu jihatdan tezkor-qidiruv tadbirlari kiberjinoyatlarning oldini olish, ularni o‘z vaqtida aniqlash va fosh etishning muhim huquqiy mexanizmi [3] sifatida namoyon bo‘lmoqda.

So‘nggi yillarda O‘zbekiston Respublikasida ham raqamli iqtisodiyotni rivojlantirish va elektron davlat boshqaruvini keng joriy etish jarayoni kiberxavfsizlik masalalarining dolzarbligini yanada oshirdi [2; 4]. Jumladan, my.gov.uz elektron hukumat portali, raqamli bank xizmatlari, onlayn to‘lov tizimlari va davlat axborot resurslaridan foydalanuvchilar soni keskin ortib bormoqda. Bu esa kiberjinoyatchilik uchun yangi kriminogen muhit shakllanishiga sabab bo‘lmoqda.

O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston – 2030” strategiyasi doirasida qabul qilgan qarorida raqamli infratuzilmani himoya qilish, kiberxavfsizlikni ta’minlash va axborot tizimlarini muhofaza qilish davlat siyosatining ustuvor yo‘nalishlaridan biri sifatida belgilangan.

Shu bilan birga, “Kiberxavfsizlik to‘g‘risida”, “Axborotlashtirish to‘g‘risida” va “Tezkor-qidiruv faoliyati to‘g‘risida”gi qonunlarda kibermakondagi huquqbuzarliklarning oldini olish va ularga qarshi kurashishga oid huquqiy normalar mustahkamlanmoqda.

Biroq, amaliyot tahlili shuni ko‘rsatmoqdaki, kiberjinoyatchilikning yuqori latentligi, elektron dalillarni yig‘ish va mustahkamlash murakkabligi, Internet tarmog‘ining transchegaraviy xususiyati, kriptografiya va anonimlashtirish texnologiyalarining keng qo‘llanilishi tezkor-qidiruv tadbirlarini amalga oshirishda muayyan huquqiy va tashkiliy muammolarni keltirib chiqarmoqda. Ayniqsa, raqamli kuzatuv, internet monitoringi, elektron ma’lumotlarni saqlash, telekommunikatsiya tarmoqlari orqali uzatiladigan axborotlarni nazorat qilish hamda sun’iy intellekt texnologiyalaridan foydalanish sohasida inson huquqlari va shaxsiy hayot daxlsizligi bilan bog‘liq huquqiy muvozanatni [1] ta’minlash dolzarb masala bo‘lib qolmoqda.

Xorijiy davlatlar tajribasi shuni ko‘rsatadiki, AQSHda Federal Bureau of Investigation va National Cyber Investigative Joint Task Force, Yevropa Ittifoqida Europol European Cybercrime Centre (EC3), Rossiya Federatsiyasida “SORM” tizimi, Janubiy Koreyada esa milliy kiberpolitsiya va raqamli tahlil markazlari orqali kiberjinoyatlarga qarshi maxsus tezkor-qidiruv mexanizmlari shakllantirilgan. Ularda elektron dalillar bilan ishlash [13], internet-monitoringi, raqamli profilling va sun’iy intellekt asosida tahlil qilish [6]tizimlari keng joriy etilgan.

Kiberjinoyatchilikning oldini olishda tezkor-qidiruv tadbirlarini huquqiy tartibga solishning kriminologik jihatlarini tahlil qilish, xorijiy davlatlar tajribasini o‘rganish hamda milliy qonunchilikni takomillashtirish bo‘yicha ilmiy asoslangan takliflar ishlab chiqish mazkur tadqiqotning dolzarbligini belgilaydi [12].

Kriminologik nuqtai nazardan, kiberjinoyatchilikning ijtimoiy xavfliligi an’anaviy jinoyat turlariga nisbatan ancha yuqori hisoblanadi [18].

Chunki bu jinoyatlar axborot-kommunikatsi texnologiyalari orqali amalga oshirilib, jamiyat, davlat va shaxs manfaatlariga bir vaqtning o‘zida katta miqdorda zarar yetkazishi mumkin. Kiberjinoyatchilikning o‘ziga xos xususiyati shundaki, u moddiy hudud bilan cheklanmaydi, virtual makonda amalga oshiriladi hamda transmilliy xarakterga ega bo‘ladi [19]. Shu sababli uni aniqlash, oldini olish va fosh etish jarayoni an’anaviy jinoyatlarga nisbatan murakkabroq hisoblanadi.

Kriminologik jihatdan kiberjinoyatchilikning xavfliligi, avvalo, qisqa vaqt ichida juda katta miqdorda moddiy zarar keltirishi [20] bilan izohlanadi. Masalan, birgina ransomware yoki bank tizimiga qilingan kiberhujum orqali millionlab foydalanuvchilarning ma’lumotlari o‘g‘irlanishi, moliyaviy tizim izdan chiqishi yoki davlat axborot resurslari faoliyati buzilishi mumkin [7; 8; 9]. Bu esa kiberjinoyatchilikni iqtisodiy xavfsizlikka tahdid soluvchi omilga aylantiradi. Ayrim holatlarda bir nafar jinoyatchi yoki kichik guruh global miqyosda minglab insonlarga zarar yetkazishi mumkinligi kiberjinoyatchilikning yuqori ijtimoiy xavfliligini ko‘rsatadi.

Kiberjinoyatchilikning yana bir muhim xususiyati jinoyatni masofadan turib sodir etish imkoniyati mavjudligidir. Jinoyatchi boshqa davlat hududida turib ham serverlarga noqonuniy kirishi, fishing xabarlar yuborishi, zararli dastur tarqatishi yoki moliyaviy firibgarlikni amalga oshirishi mumkin. Bu

esa hududiy yurisdiksiya, ekstraditsiya va xalqaro huquqiy yordam masalalarini murakkablashtiradi. Shu nuqtai nazardan kiberjinoyatchilik transmilliy uyushgan jinoyatchilikning yangi ko‘rinishi sifatida baholanmoqda.

Kriminologiyada jinoyatning latentligi muhim tushunchalardan biri hisoblanadi. Kiberjinoyatchilikda latentlik darajasi juda yuqori bo‘lib, ko‘plab holatlarda jabrlanuvchilar jinoyat haqida huquqni muhofaza qiluvchi organlarga murojaat qilmaydi [17]. Buning sabablari sifatida tashkilotlar o‘z nufuziga putur yetishidan qo‘rqishi, shaxsiy ma’lumotlar tarqalishidan xavotirlanish, jinoyatni aniqlash imkoniyati pastligiga ishonchsizlik kabi omillarni ko‘rsatish mumkin. Ayniqsa, elektron dalillarning tez o‘zgarishi yoki yo‘q qilinishi jinoyatni isbotlash jarayonini yanada qiyinlashtiradi.

Kiberjinoyatchilikning xavfli jihatlaridan biri anonimlik darajasining yuqoriligidir. VPN, proxy, darknet, kriptovalyuta va anonim messenjerlardan foydalanish jinoyatchining shaxsini aniqlashni qiyinlashtiradi. Bu esa kriminologiyada “kiberdeviatsiya” tushunchasining shakllanishiga olib kelmoqda [10]. Ya’ni inson real hayotda sodir eta olmaydigan yoki javobgarlikdan qo‘rqib amalga oshirmaydigan harakatlarni virtual muhitda oson amalga oshirishga intiladi. Anonimlik hissi shaxsning ijtimoiy nazoratdan chiqishiga va deviant xulqning kuchayishiga sabab bo‘ladi.

Viktimologiya nuqtai nazaridan ham kiberjinoyatchilikning xavfliligi yuqori hisoblanadi. Chunki Internet foydalanuvchilari, ayniqsa yoshlar, talabalar, qariyalar va raqamli savodxonligi past shaxslar kiberjinoyatchilar uchun oson “nishon”ga aylanmoqda. Ijtimoiy tarmoqlar orqali aldash, onlayn firibgarlik, fishing, kiberbulling, shaxsiy ma’lumotlarni tarqatish kabi harakatlar inson psixologiyasiga ham jiddiy ta’sir ko‘rsatmoqda. Shu sababli zamonaviy kriminologiyada “kiberviktimologiya” yo‘nalishi alohida shakllanib bormoqda [10].

Zamonaviy sharoitda kiberjinoyatchilikka qarshi kurashish faqat jazolash orqali emas, balki uning sabab va shart-sharoitlarini aniqlash, kriminogen omillarni bartaraf etish hamda profilaktika choralarini kuchaytirish orqali amalga oshirilishi lozim[11]. Kriminologik profilaktika raqamli muhitda axborot xavfsizligini kuchaytirish, aholining kiberhuquqiy madaniyatini oshirish, davlat organlari va internet provayderlarining hamkorligini ta’minlash, raqamli monitoring tizimlarini takomillashtirish kabi choralarni o‘z ichiga oladi.

Ma’lumki, tezkor-qidiruv tadbirlarini o‘tkazish kiberjinoyatchilikka qarshi kurashishning muhim kriminologik mexanizmi hisoblanadi. Chunki mazkur tadbirlar nafaqat jinoyatni fosh etish, balki uning oldini olish, jinoyat sodir etishga moyil shaxslarni aniqlash, kriminogen muhitni tahlil qilish, Internet tarmoqlaridagi shubhali faollikni monitoring qilish hamda jinoyat xavfini prognozlash imkonini beradi. Ayniqsa, raqamli kuzatuv, Internet monitoringi, telekommunikatsiya tarmoqlari orqali uzatiladigan axborotlarni tahlil qilish, elektron dalillarni tezkor mustahkamlash, sun’iy intellekt asosida xavflarni aniqlash kabi mexanizmlar zamonaviy tezkor-qidiruv faoliyatining muhim elementlariga aylanmoqda.

Xorijiy davlatlar amaliyotida kiberjinoyatchilik profilaktikasida tezkor-qidiruv tadbirlariga alohida e’tibor qaratilmoqda. Xususan, AQSHda Federal Bureau of Investigation hamda National Cyber Investigative Joint Task Force, Yevropa Ittifoqida Europol European Cybercrime Centre (EC3), Rossiya Federatsiyasida SORM tizimi, Janubiy Koreyada esa milliy kiberpolitsiya va raqamli tahlil markazlari orqali Internet monitoringi, raqamli profilling va elektron kuzatuv mexanizmlari keng qo‘llanilmoqda.

Bu esa tezkor-qidiruv tadbirlarining kiberjinoyatchilikning oldini olishdagi ahamiyati tobora ortib borayotganini ko‘rsatadi.

Zamonaviy kriminologiya fanida jinoyatchilikni tadqiq etishda jinoyatning sabab va shart-sharoitlari, jinoyatchining shaxsi, viktimologik omillar hamda profilaktika mexanizmlarini tahlil qilish muhim ahamiyat kasb etadi. Kiberjinoyatchilik axborot-kommunikatsiya texnologiyalari orqali sodir etiladigan, yuqori latentlikka, transmilliy xususiyatga va tez o‘zgaruvchan dinamikaga ega bo‘lgan jinoyat turi sifatida [11] zamonaviy kriminologiyaning dolzarb tadqiqot obyektlaridan biriga aylanmoqda.

An’anaviy jinoyatlardan farqli ravishda kiberjinoyatchilik virtual muhitda amalga oshirilishi, anonimlik imkoniyatining yuqoriligi, elektron dalillarning tez o‘zgarishi yoki yo‘q qilinishi hamda jinoyatni masofadan turib sodir etish imkoniyati

bilan ajralib turadi. Shu bois mazkur jinoyatlarni tahlil qilishda klassik kriminologik yondashuvlar bilan bir qatorda, raqamli kriminologiya, kiberviktimologiya va axborot xavfsizligi sohalari bilan integratsiyalashgan yondashuvlar ham muhim ahamiyat kasb etadi[16].

Kriminologik nuqtai nazardan kiberjinoyatchilikning shakllanishiga turli ijtimoiy, texnik, psixologik va iqtisodiy omillar ta’sir ko‘rsatadi. Mazkur omillar o‘zaro bog‘liq holda kibermakonda kriminogen muhitni yuzaga keltiradi hamda jinoyat sodir etish ehtimolini oshiradi.

Kiberjinoyatchilikning sabab va shart sharoitlari quyidagi omillar bilan bog‘liq

Ijtimoiy omillar. Kiberjinoyatchilikning kelib chiqishiga ta’sir qiluvchi asosiy omillardan biri ijtimoiy muhit hisoblanadi. Internet texnologiyalarining ommalashuvi, ijtimoiy tarmoqlardan keng foydalanish va raqamli xizmatlarning hayotning barcha sohalariga kirib borishi insonlarning virtual muhitga bog‘liqligini kuchaytirmoqda. Ayniqsa, yoshlar o‘rtasida Internetdan nazoratsiz va uzoq vaqt foydalanish holatlari kiberdeviant xulq-atvorning shakllanishiga sabab bo‘lmoqda.

Kriminologik tadqiqotlarga ko‘ra, raqamli madaniyat va kiberhuquqiy savodxonlikning yetarli emasligi fishing, onlayn firibgarlik, ijtimoiy tarmoqlar orqali aldash kabi jinoyatlarning ko‘payishiga olib kelmoqda. Shuningdek, ishsizlik, ijtimoiy tengsizlik va tez boyish istagi ayrim shaxslarni kiberjinoyatchilik orqali daromad topishga undashi mumkin. Ayniqsa, darknet platformalari, kriptovalyuta bozorlari va noqonuniy onlayn xizmatlar virtual jinoiy iqtisodiyotning shakllanishiga sabab bo‘lmoqda [14; 15].

Xorijiy tadqiqotlarda ta’kidlanishicha, pandemiyadan keyin masofaviy ishlash va onlayn ta’limning kengayishi kiberjinoyatchilik uchun yangi imkoniyatlar yaratgan. Bu esa kiberjinoyatchilikning ijtimoiy xavfliligini yanada oshirgan.

Texnik omillar. Kiberjinoyatchilikning yuzaga kelishida texnik omillar ham muhim o‘rin tutadi. Axborot tizimlaridagi dasturiy va texnik zaifliklar, himoya mexanizmlarining yetarli darajada emasligi, zaif parollardan foydalanish, litsenzion bo‘lmagan dasturlardan foydalanish va kiberxavfsizlik talablariga rioya qilinmasligi jinoyat sodir etish uchun qulay shart-sharoit yaratadi. Ko‘plab tashkilotlarda axborot xavfsizligi siyosati yetarlicha shakllanmaganligi sababli serverlarga noqonuniy kirish, ma’lumotlarni o‘g‘irlash, zararli dastur joylashtirish va ransomware hujumlari sodir etilmoqda. Ayniqsa, davlat axborot tizimlari, bank-moliya sektorlari va elektron hukumat platformalariga qilingan kiberhujumlar milliy xavfsizlikka jiddiy tahdid tug‘dirmoqda.

Kriminologik nuqtai nazardan texnik zaifliklar “kriminogen imkoniyat” sifatida baholanadi. Ya’ni jinoyatchi texnik himoyaning yetarli emasligidan foydalanib, jinoyat sodir etish imkoniyatiga ega bo‘ladi. Shu sababli axborot tizimlarini muntazam audit qilish, kiberxavfsizlik standartlarini joriy etish va raqamli himoya mexanizmlarini kuchaytirish profilaktikaning muhim yo‘nalishlaridan biri hisoblanadi.

Psixologik omillar. Kiberjinoyatchilikning kelib chiqishida psixologik omillar ham muhim ahamiyat kasb etadi. Virtual muhitda anonimlikning mavjudligi, shaxsning o‘zini “ko‘rinmas” deb his qilishi va jazodan qochib qolish mumkinligi haqidagi tasavvur ayrim shaxslarda deviant xulq-atvorni kuchaytiradi. Kriminologiyada mazkur holat “onlayn dezingibitsiya effekti” deb ataladi. Ya’ni inson real hayotda sodir etmasligi mumkin bo‘lgan harakatlarni Internet muhitida oson amalga oshirishga moyil bo‘ladi. Anonimlik hissi shaxsning ijtimoiy nazoratdan chiqishiga, huquqiy mas’uliyatni kam his qilishiga va agressiv yoki firibgarlikka moyil xatti-harakatlarning kuchayishiga olib keladi. Shuningdek, ba’zi hollarda kiberjinoyatchilik “o‘yin” yoki “texnik tajriba” sifatida qabul qilinishi ham kuzatiladi. Xususan, yoshlar orasida xakerlikni “obro‘” yoki “intellektual ustunlik” belgisi sifatida qabul qilish holatlari uchraydi. Bu esa kiberjinoyatchilik profilaktikasida psixologik va tarbiyaviy choralarni kuchaytirish zarurligini ko‘rsatadi.

Iqtisodiy omillar. Kiberjinoyatchilikning keng tarqalishiga iqtisodiy manfaatdorlik ham katta ta’sir ko‘rsatmoqda. Internet orqali qisqa vaqt ichida katta miqdorda noqonuniy daromad olish imkoniyati kiberjinoyatchilar uchun motivatsiya hisoblanadi. Fishing, internet-banking firibgarligi, kriptovalyuta orqali pul yuvish, onlayn tovlamachilik, zararli dasturlar tarqatish va elektron to‘lov tizimlariga hujum qilish orqali jinoyatchilar katta miqdorda daromad topmoqda. Ayniqsa, kriptova-

lyutalarning anonim xususiyati ayrim hollarda noqonuniy moliyaviy operatsiyalarni amalga oshirish uchun qulay vositaga aylanmoqda. Xalqaro tashkilotlar ma'lumotlariga ko'ra, kiberjinoyatchilik global "soyaviy raqamli iqtisodiyot"ning muhim qismiga aylanib bormoqda. Bu esa mazkur jinoyat turini uyushgan transmilliy jinoyatchilik bilan bog'liq holda o'rganishni talab etadi.

Kriminologiya fanida profilaktika jinoyat sodir bo'lishidan oldin kriminogen omillarni aniqlash, xavf darajasini baholash va jinoyatni keltirib chiqaruvchi shart-sharoitlarni bartaraf etishga qaratilgan faoliyat sifatida tushuniladi. Kibermakonda mazkur vazifalarni amalga oshirishda tezkor-qidiruv tadbirlari muhim o'rin tutadi. Chunki internet muhitida jinoyatchilarning harakatlari, jinoiy guruhlar faoliyati, zararli dasturlar tarqalishi va noqonuniy axborot almashinuvi an'anaviy jinoyatchilikka nisbatan tezkor va yashirin shaklda amalga oshiriladi.

Tezkor-qidiruv tadbirlarining kriminologik ahamiyati, avvalo, kibermakondagi kriminogen vaziyatni muntazam monitoring qilish imkoniyati bilan izohlanadi. Internet tarmoqlari, ijtimoiy platformalar, forumlar, darknet segmentlari va kriptovalyuta maydonlarini tahlil qilish orqali kiberjinoyatchilikning yangi tendensiyalari, uyushgan kiberguruhlar faoliyati va xavf darajasi yuqori bo'lgan segmentlar aniqlanadi. Bu esa huquqni muhofaza qiluvchi organlarga jinoyat sodir bo'lishidan avval profilaktik choralarni ko'rish imkonini beradi.

Kriminologik nuqtai nazardan tezkor-qidiruv tadbirlari jinoyatchilik tendensiyalarini prognoz qilish vazifasini ham bajaradi. Masalan, ma'lum vaqt oralig'ida fishing hujumlari, bank kartalari ma'lumotlarini o'g'irlash yoki ransomware hujumlarining ko'payishi muayyan jinoiy guruhlar faollashganligini ko'rsatishi mumkin. Mazkur ma'lumotlar tahlili asosida xavfli sohalar belgilanib, profilaktika choralari kuchaytiriladi. Shu jihatdan tezkor-qidiruv tahlili kriminologik prognozlashning muhim elementi hisoblanadi.

Shuningdek, tezkor-qidiruv tadbirlari orqali kiberjinoyatchilarning ijtimoiy va psixologik xususiyatlari ham o'rganiladi. Kriminologiyada jinoyatchining shaxsini tahlil qilish profilaktikaning muhim sharti hisoblanadi. Kiberjinoyatchilik sohasida mazkur tahlil raqamli muhitdagi xatti-harakatlar, onlayn muloqot, virtual aloqalar va internet faolligi orqali amalga oshiriladi. Bu esa kiberjinoyatchilarning kriminologik profilini shakllantirish imkonini beradi.

Kiberjinoyatchilik profilaktikasida viktimologik tahlil ham muhim ahamiyatga ega. Tezkor-qidiruv tadbirlari orqali qaysi ijtimoiy guruh yoki internet foydalanuvchilari kiberjinoyatlar ta'siriga ko'proq uchrayotganligi tezkor aniqlanadi. Masalan, yoshlar, keksalar, raqamli savodxonligi past foydalanuvchilar yoki onlayn to'lov tizimlaridan faol foydalanuvchilar viktimlik xavfi yuqori bo'lgan toifa sifatida baholanishi mumkin. Bu esa maqsadli profilaktika choralarini ishlab chiqish imkonini beradi.

Kiberjinoyatchilikning oldini olishda *ma'lumotlar to'plash* hamda *tezkor kuzatuv* tezkor-qidiruv tadbirlariga tayangan holda quyidagi chora-tadbirlar o'tkaziladi.

1.Kiberjinoyatchilikning oldini olishda Internet monitoringi eng muhim chora hisoblanadi. Internet monitoringi orqali huquqni muhofaza qiluvchi organlar ochiq va yopiq tarmoq segmentlaridagi jinoiy faollikni kuzatish, tahlil qilish va baholash imkoniyatiga ega bo'ladilar. Internet monitoringi orqali darknet platformalari, fishing saytlar, zararli dastur tarqatuvchi manbalar, botnet tarmoqlari, noqonuniy kriptovalyuta operatsiyalari, ekstremistik, terroristik kontentlar aniqlanmoqda. Ayniqsa, darknet muhitida narkotik vositalar savdosi, shaxsiy ma'lumotlar savdosi, zararli dasturlar sotuvi va kiberhujum xizmatlari keng tarqalgani kuzatilmoqda.

Internet monitoringi kriminologik jihatdan jinoyatchilikning yashirin shakllarini aniqlash, kriminogen muhitni baholash va jinoyatchilarning virtual aloqalarini tahlil qilish imkonini beradi. Shu bilan birga, mazkur monitoring profilaktik funksiyani ham bajaradi, chunki huquqni muhofaza qiluvchi organlarning doimiy raqamli nazorati jinoyat sodir etish ehtimolini pasaytiruvchi omil sifatida ta'sir ko'rsatadi.

2.Raqamli profayling – bu kiberjinoyatchilarning Internet muhitidagi xatti-harakatlari, onlayn faolligi, muloqot uslubi, texnik harakatlari va raqamli izlari asosida ularning kriminologik profilini shakllantirish jarayoni. Kriminologiyada jinoyatchining shaxsini o'rganish muhim ahamiyatga ega bo'lgani kabi kiberjinoyatchilikda ham raqamli profayling profilaktika va tezkor-qidiruv faoliyatining muhim elementi hisoblanadi. Masalan, muayyan shaxsning qaysi forumlarda ishtirok etishi, qanday zararli dasturlardan foydalanishi, qaysi kriptovalyuta hamyonlari bilan aloqada bo'lishi yoki qaysi IP-manzillar orqali faoliyat yuritishi uning kriminologik profilini shakllantirish imkonini beradi.

Raqamli profayling orqali jinoyat sodir etishga moyil shaxslar, uyushgan kiberguruhlar va xavfli virtual aloqalar aniqlanadi. Bu esa jinoyatni erta bosqichda aniqlash va profilaktika choralarini ko'rish imkonini beradi. Shu bilan birga, raqamli profayling sun'iy intellekt va Big Data texnologiyalari bilan integratsiya qilinganda uning samaradorligi yanada oshadi.

3.Kiberjinoyatni oldindan prognoz qilish. Kiberjinoyatchilikka qarshi kurashishda predictive policing texnologiyalari keng qo'llanilmoqda. Mazkur tizimlar sun'iy intellekt, mashinali o'qitish (machine learning) va Big Data tahlili asosida ishlaydi.

Predictive policing tizimlari Internet tarmoqlaridagi shubhali faollik, fishing hujumlari, zararli dasturlar tarqalishi, botnet harakatlari va kriptovalyuta operatsiyalarini tahlil qilib, qaysi sohada yoki qaysi vaqtda kiberjinoyat sodir etilishi ehtimoli yuqori ekanligini aniqlaydi. Bu esa huquqni muhofaza qiluvchi organlarga tezkor profilaktika choralarini ko'rish imkonini beradi.

Kriminologik nuqtai nazardan predictive policing jinoyatchilikning dinamikasini tahlil qilish, kriminogen omillarni baholash va jinoyat xavfini prognoz qilishning zamonaviy usuli hisoblanadi. Shu bilan birga, mazkur texnologiyalar inson omili bilan bog'liq xatolarni qisqartirish, tezkor ma'lumotlarni real vaqt rejimida tahlil qilish va xavfli tendensiyalarni erta bosqichda aniqlash imkonini beradi. Biroq kiberjinoyatni oldindan prognoz qilish texnologiyalarini qo'llash inson huquqlari, shaxsiy hayot daxlsizligi va raqamli kuzatuvning huquqiy chegaralari bilan bog'liq muammolarni ham keltirib chiqarmoqda. Shu sababli mazkur texnologiyalarni qo'llashda qonuniylik, shaffoflik prinsiplariga qat'iy rioya qilinishi talab etiladi.

Kiberjinoyatchilikning oldini olishda tezkor-qidiruv tadbirlarini huquqiy tartibga solishga oid amaliyotlarda bir qator muammolar kuzatiladi.

Birinchidan, kiberjinoyatchilikning transmilliy xususiyati tezkor-qidiruv tadbirlarini milliy qonunchilik doirasida amalga oshirish imkoniyatlarini cheklaydi. Jinoyatchi bir davlatda, server ikkinchi davlatda, jabrlanuvchi esa uchinchi davlatda joylashgan holatlarda elektron dalillarni tezkor olish, saqlash va protsessual rasmiylashtirish murakkablashadi.

Ikkinchidan, tezkor-qidiruv tadbirlarini raqamli muhitda qo'llashning aniq huquqiy chegaralari yetarlicha belgilab berilmagan. Internet monitoringi, elektron yozishmalarni kuzatish, IP - manzillarni aniqlash, raqamli profayling kabi choralar amaliyotda inson huquqlari, shaxsiy hayot daxlsizligi va ma'lumotlar muhofazasi bilan to'qnash kelishi mumkin.

Uchinchidan, elektron dalillar bilan ishlashda yagona kriminalistik va protsessual standartlarning yetarli shakllanmagani kiberjinoyatlarni fosh etish samaradorligini pasaytiradi. Raqamli izlar tez o'chirilishi, o'zgartirilishi yoki xorijiy serverlarda saqlanishi sababli ularning ishonchliligi va maqbulligini ta'minlash murakkab hisoblanadi.

To'rtinchidan, kiberjinoyatchilikning kriminologik profilaktikasi yetarli darajada tizimlashtirilmagan. Amaliyotda asosiy e'tibor jinoyat sodir etilgandan keyin uni fosh etishga qaratiladi, biroq kiberjinoyatlarning sabablari, shart-sharoitlari, jinoyatchi shaxsi, viktimologik omillar va raqamli muhitdagi kriminogen xavflar chuqur o'rganilmaydi.

Beshinchidan, tezkor-qidiruv faoliyatini amalga oshiruvchi organlarning zamonaviy raqamli texnologiyalardan foydalanish salohiyati barcha holatlarda yetarli emas. Sun'iy intellekt, Big Data tahlili, darknet monitoringi, kriptovalyuta tranzaksiyalarini kuzatish, kibertahdidlarni prognoz qilish kabi vositalarni qo'llash bo'yicha huquqiy, tashkiliy va kadrlar bilan bog'liq muammolar mavjud.

Yuqorida ta'kidlab o'tilgan real muammolarni bartaraf etish yuzasidan quyidagilar taklif etiladi:

birinchidan, kiberjinoyatchilikka qarshi kurashishda tezkor-qidiruv tadbirlarini xalqaro hamkorlik mexanizmlari bilan uyg'unlashtirish zarur. Kiberjinoyatchilikning asosiy xususiyatlaridan biri – uning transmilliy tabiatga ega ekanligi. Amaliyotda kiberjinoyatchi bir davlat hududida turib, ikkinchi davlat serverlaridan foydalanishi, jabrlanuvchi esa uchinchi davlat fuqarosi bo'lishi mumkin. Bunday sharoitda jinoyatni fosh etish va elektron dalillarni yig'ish faqat milliy huquqiy mexanizmlar doirasida

KRIMINOLOGIK TAHLIL VA NAZARIY-METODOLOGIK YONDASHUV

samarali amalga oshirilmaydi. Masalan, fishing orqali bank kartalari ma'lumotlarini o'g'irlash jinoyatlarida serverlar Niderlandiya yoki Germaniyada, VPN xizmatlari Kanadada, kriptovalyuta hamyonlari esa Singapurda joylashgan bo'lishi mumkin. Bu holatda tezkor-qidiruv faoliyatini amalga oshiruvchi organlar xorijiy davlatlar bilan tezkor axborot almashmas ekan, elektron dalillar qisqa vaqt ichida o'chirilishi yoki boshqa serverlarga ko'chirilishi ehtimoli yuqori bo'ladi. Shu sababli elektron dalillarni transchegaraviy tartibda olish, cloud serverlardan ma'lumot so'rash, IP-manzil va log-fayllarni aniqlash, kriptovalyuta operatsiyalarini kuzatish, internet-provayderlar bilan xalqaro hamkorlik qilish mexanizmlarini huquqiy jihatdan mustahkamlash zarur;

ikkinchidan, raqamli muhitda amalga oshiriladigan tezkor-qidiruv tadbirlarining huquqiy chegaralarini aniq belgilash lozim. Kibermakonda amalga oshiriladigan tezkor-qidiruv tadbirlari inson huquqlari bilan bevosita bog'liq hisoblanadi. Internet monitoringi, elektron xat-xabarlarni kuzatish, ijtimoiy tarmoqlarni tahlil qilish yoki raqamli profayling jarayonida shaxsiy hayot daxlsizligi buzilishi xavfi yuzaga keladi. Masalan, sud sanksiyasiz shaxsning telegram yozishmalari, elektron pochtalari, ijtimoiy tarmoq faolligi, geolokatsiya ma'lumotlari kuzatilishi inson huquqlariga aralashuv sifatida baholanishi mumkin. Shu bois tezkor-qidiruv tadbirlarining huquqiy chegaralari aniq belgilanishi zarur;

uchinchidan, elektron dalillar bilan ishlashning yagona milliy standartini ishlab chiqish zarur. Kiberjinoyatlarni tergov qilishda elektron dalillar hal qiluvchi ahamiyatga ega hisoblanadi. Biroq raqamli dalillar oddiy moddiy dalillardan farq qilib, oson o'zgarishi, o'chirilishi yoki soxtalashtirilishi mumkin. Masalan, server loglari, IP-manzillar, elektron xatlar, Telegram yozishmalari, blockchain tranzaksiyalari, CCTV cloud arxivlari, elektron dalil sifatida qo'llaniladi. Agar ushbu dalillar protsessual talablarga rioya qilinmasdan olinsa, sud ularni maqbul dalil sifatida tan olmasligi mumkin. Buning uchun elektron dalillarni yig'ish, hash-kod orqali aslligini tekshirish va saqlash, ekspertizadan o'tkazish bo'yicha yagona milliy standart ishlab chiqish zarur;

to'rtinchidan, kiberjinoyatchilik profilaktikasiga kriminologik yondashuvni kuchaytirish maqsadga muvofiq. Amaliyotda aksariyat hollarda kiberjinoyat sodir etilgandan keyin chora ko'riladi. Biroq kriminologiya fani jinoyatning oldini olishga asosiy e'tibor qaratadi. Shu nuqtai nazardan kiberjinoyatchilikning sabablari, raqamli muhitdagi kriminogen omillar, jinoyatchi shaxsini xususiyatlari, internet foydalanuvchilarining viktimologik holati, doimiy tahlil qilinishi lozim. Masalan, yoshlar o'rtasida onlayn qimor, kriptovalyuta orqali firibgarlik, kiberbulling holatlarining o'sishi profilaktik choralarni kuchaytirish zarurligini ko'rsatadi.

Xulosa qilib aytganda, kiberjinoyatchilik zamonaviy raqamli jamiyatning eng xavfli transmilliy tahdidlaridan biri hisoblanadi. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, Internetdan ommaviy foydalanish, elektron to'lov tizimlari, cloud texnologiyalari, kriptovalyuta va sun'iy intellektning keng qo'llanilishi kiberjinoyatchilikning yangi shakl va usullarini yuzaga keltirmoqda. Bu esa tezkor-qidiruv faoliyatini raqamli muhit xususiyatlariga mos ravishda takomillashtirish zaruratini keltirib chiqarmoqda.

Xorijiy davlatlar tajribasi tahlili shuni ko'rsatdiki, AQSH, Rossiya Federatsiyasi va Janubiy Koreyada kiberjinoyatchilikka qarshi kurashishda tezkor-qidiruv tadbirlarining huquqiy asoslari aniq belgilangan bo'lib, elektron dalillar bilan ishlash, transchegaraviy hamkorlik, raqamli monitoring va kiberprofilaktika tizimlari samarali yo'lga qo'yilgan. Ayniqsa, Budapesht konvensiyasi doirasidagi xalqaro hamkorlik mexanizmlari kiberjinoyatlarni tezkor aniqlash va elektron dalillar almashinuvini ta'minlashda muhim ahamiyat kasb etmoqda.

Shu bilan birga, kiberjinoyatchilikka qarshi kurashish jarayonida inson huquqlari va shaxsiy hayot daxlsizligini ta'minlash dolzarb masala bo'lib qolmoqda. Shu sababli raqamli muhitda amalga oshiriladigan tezkor-qidiruv tadbirlari qonuniylik, sud nazorati, inson huquqlarini himoya qilish prinsiplari asosida amalga oshirilishi lozim.

Umuman olganda, kiberjinoyatchilikning oldini olishda tezkor-qidiruv tadbirlarini huquqiy tartibga solish sohasini takomillashtirish raqamli xavfsizlikni ta'minlash, inson huquqlarini himoya qilish, jamiyat va davlat manfaatlarini saqlash hamda kibermakonda qonuniylikni mustahkamlashning muhim sharti hisoblanadi.

Foydalanilgan manbalar

1. O'zbekiston Respublikasining 2023-yil 30-aprelda qabul qilingan yangi tahrirdagi Konstitutsiyasi // URL: http: // www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 05.05.2026).
2. O'zbekiston Respublikasining 2003-yil 11-dekabrda qabul qilingan "Axborotlashtirish to'g'risida"gi 560-II-son qonuni // Elektron manba: URL: http:// www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 06.05.2026).
3. O'zbekiston Respublikasining 2012-yil 25-dekabrda qabul qilingan "Tezkor-qidiruv faoliyati to'g'risida"gi O'RQ-344-son qonuni // Elektron manba: URL: http:// www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 07.05.2026).
4. O'zbekiston Respublikasining 2022-yil 15-aprelda qabul qilingan "Kiberxavfsizlik to'g'risida"gi O'RQ-764-son qonuni // Elektron manba: URL: http:// www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 08.05.2026).
5. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi PF-6079-son "Raqamli O'zbekiston – 2030 strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi farmoni // URL: http:// www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 09.05.2026).
6.O'zbekiston Respublikasi Prezidentining 2021-yil 17-fevralda qabul qilgan "Sun'iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to'g'risida"gi PQ-4996-son qarori// URL: http:// www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 10.05.2026).
7.Бастрыкин А.И. Расследование преступлений в сфере компьютерной информаци. – Санкт-Петербург: Юридический центр, 2021. – 368 с.
8.Brenner S.W. Cybercrime and the Law: Challenges, Issues and Outcomes. — Boston: Northeastern University Press, 2012. – URL: https://aspenpublishing.com (Электрон манбага мурожаат қилинган вақт: 11.05.2026).
9. Federal Bureau of Investigation. Internet Crime Report 2024. — URL: https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report (Электрон манбага мурожаат қилинган вақт: 12.05.2026).
10.Ismailov I., Ziyodullayev M. Kriminologiya: Darslik. – Toshkent: O'zbekiston Respublikasi IIV Akademiyasi, 2019. – 496 b.
11.Каримов М.М. Кибержиноятчилик профилактикасининг криминологик муаммолари. – Тошкент: Янги аср авлоди, 2020. – 276 б.
12.Лунеев В.В. Криминология: Учебник. – Москва: Юрайт, 2020. — 686 с.
13.Мирзаев У.Т. Тезкор-қидирув фаолиятида электрон далиллар билан ишлашнинг процессуал хусусиятлари. – Тошкент: Ўзбекистон Республикаси ИИВ Академияси, 2023. – 224 б.
14. Россинская Е.Р. Судебная компьютерно-техническая экспертиза. – Москва: Норма, 2022. – 344 с.
15.Рустамбаев М.Х. Ўзбекистон Республикаси Жиноят ҳуқуқи курси. Том 5. Ахборот технологиялари соҳасидаги жиноятлар. – Тошкент: ИЛМ ЗИЁ, 2021. – 384 б.
16.Саидов А.Х., Очилов Б. Ахборот хавфсизлиги ва киберҳуқуқ муаммолари. – Тошкент: Адолат, 2021. – 312 б.
17.Турсунов А.С. Кибержиноятчиликка қарши курашишнинг ҳуқуқий ва ташкилий асослари. – Тошкент: ТДЮ нашриёти, 2022. – 268 б.
18.Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2007. – 278 p. – ISBN: 978-0745630636. – URL: https://www.amazon.com/Cybercrime-Transformation-Crime-Information-Age/dp/0745627366 (Электрон манбага мурожаат қилинган вақт: 06.12.2021).
19. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. — Cambridge: Polity Press, 2007. — URL: https://papers.ssrn.com/sol3/ papers.cfm? abstract_id=1066922 (Электрон манбага мурожаат қилинган вақт: 13.05.2026).
20. Yar M. Cybercrime and Society.; Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. — URL: https://uob.edu.ly/ (Электрон манбага мурожаат қилинган вақт: 14.05.2026).