KIBERJINOYAT VA AN’ANAVIY JINOYAT: O‘XSHASHLIKLAR, FARQLAR VA HUQUQIY CHEGARALAR

Abdullayeva Saidaxon Ganjabay qizi
Toshkent davlat yuridik universiteti Kiber huquqi yo‘nalishi magistranti

Annotatsiya. *Maqolada kiberjinoyat va an’anaviy jinoyat o‘rtasidagi o‘xshashliklar, farqlar hamda ularni huquqiy kvalifikatsiya qilish chegaralari tadqiq etiladi. Normativ-huquqiy, qiyosiy-huquqiy va sud amaliyotini tahlil qilish usullari asosida raqamli texnologiya jinoyatda tajovuz obyekti, sodir etish vositasi yoki aloqa muhiti bo‘lishi mumkinligi ko‘rsatildi. Vobkent tuman sudi amaliyoti, Morris va Van Buren ishlarining tahlili texnologiyadan foydalanish fakti jinoyat tarkibining maxsus belgilarini o‘z-o‘zidan isbotlamasligini namoyish etadi. Kvalifikatsiya mezonlarini aniqlashtirish, elektron dalillarni saqlash tartibini takomillashtirish va transchegaraviy hamkorlikni qonuniy asosda kuchaytirish taklif etiladi.*

Kalit so‘zlar: *kiberjinoyat, an’anaviy jinoyat, jinoyat tarkibi, huquqiy kvalifikatsiya, elektron dalillar, yurisdiksiya, raqamli texnologiyalar.*

Аннотация. *В статье исследуются сходства, различия и правовые границы квалификации киберпреступлений и традиционных преступлений. На основе формально-юридического и сравнительно-правового методов, а также анализа судебной практики показано, что цифровая технология может выступать объектом посягательства, средством совершения преступления либо средой коммуникации. Анализ дела Вобкентского районного суда, а также дел Morris и Van Buren демонстрирует, что сам факт применения технологии не доказывает специальных признаков состава преступления. Предлагается уточнить критерии квалификации, совершенствовать правила сохранения электронных доказательств и развивать международное сотрудничество при соблюдении процессуальных гарантий.*

Ключевые слова: *киберпреступление, традиционное преступление, состав преступления, правовая квалификация, электронные доказательства, юрисдикция, цифровые технологии.*

KIRISH

Mavzuning dolzarbligi raqamli infratuzilmaning kundalik iqtisodiy va ijtimoiy munosabatlarga chuqur kirib borishi bilan belgilanadi. Bank operatsiyalari, davlat xizmatlari, elektron savdo va shaxslararo muloqotning onlayn shaklga o‘tishi jinoyat sodir etishning yangi imkoniyatlarini yuzaga keltirdi. Biroq huquqiy muammo texnologiyaning

mavjudligidagina emas: jinoyatning bevosita obyekti, aybdorning harakat usuli, zarar kelib chiqish mexanizmi va dalillarning xususiyatini aniq ajratish zarur. Ayniqsa, oddiy firibgarlikning messenjer orqali sodir etilishi bilan axborot tizimiga ruxsatsiz kirish orqali mablag‘ egallanishi bir xil huquqiy hodisa emas. Mazkur farqni e’tiborsiz qoldirish jinoyatni noto‘g‘ri kvalifikatsiya qilish, bir xil holatlarga turlicha huquqiy baho berish va elektron dalillarni baholashda xatolarga olib kelishi mumkin.

Tadqiqotning maqsadi – an’anaviy jinoyat va kiberjinoyat o‘rtasidagi moddiy-huquqiy hamda protsessual farqlarni izchil mezonlarga ajratish, mavjud normalarning tatbiq chegaralarini aniqlash va sud amaliyoti uchun asoslangan tavsiyalar taklif etish. Asosiy savollar raqamli vosita qachon jinoyatning mustaqil belgisi bo‘lishi, masofaviylik va avtomatlashtirish xavflilikni qanday o‘zgartirishi, elektron dalilni tekshirish hamda xalqaro hamkorlik va shaxs huquqlari muvozanati bilan bog‘liq.

Tadqiqotning ilmiy yangiligi raqamli texnologiyaning jinoyatdagi rolini uch mezon orqali baholash taklifida ifodalanadi: texnologiya tajovuzning mustaqil obyekti bo‘lishi; u an’anaviy jinoyatni sodir etish vositasi sifatida xizmat qilishi; raqamli muhit faqat aloqa yoki dalilni qayd etish sharoiti bo‘lib qolishi. Mazkur uchlik jinoyat tarkibi belgilarini aniqlash uchun tahliliy model sifatida qo‘llanadi.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Kiberjinoyat va an’anaviy jinoyatning o‘zaro munosabati ilmiy adabiyotlarda bir xil izohlanmaydi. Tadqiqotlarning bir yo‘nalishi raqamli texnologiyalar jinoyatning ko‘lami va tashkiliy tuzilishini o‘zgartirishiga urg‘u bersa, boshqa yo‘nalish jinoyat tarkibining huquqiy belgilarini birlamchi mezon sifatida ko‘radi.

D. S. Wall «Cybercrime: The Transformation of Crime in the Information Age» (2007) asarida tarmoq texnologiyalari jinoyat sodir etish imkoniyatlarini sifat jihatidan o‘zgartirayotganini asoslaydi. Uning fikricha, avtomatlashtirish, keng miqyosda takrorlash va ko‘plab jabrlanuvchilarga bir vaqtda ta’sir ko‘rsatish kiberjinoyatning muhim kriminologik xususiyatlaridir. Bu qarash jinoyatning ijtimoiy xavfliligini tushuntiradi, biroq muayyan qilmishni huquqiy kvalifikatsiya qilish uchun texnologik ko‘lamning o‘zi yetarli emas: jinoyat tarkibining qonunda belgilangan alomatlari ham isbotlanishi zarur [3].

J. Clough «Principles of Cybercrime» (2015) tadqiqotida kiberjinoyatlarga jinoyat huquqi normalari va sud amaliyoti nuqtayi nazaridan yondashib, kompyuter tizimiga qaratilgan tajovuzlar, firibgarlik bilan bog‘liq qilmishlar, shaxsga qarshi huquqbuzarliklar va yurisdiksiya masalalarini alohida tahlil qiladi. Uning doktrinal yondashuvi raqamli muhitda sodir etilgan har qanday noqonuniy harakatni avtomatik tarzda alohida kiberjinoyat deb hisoblamaslik, balki uning huquqiy tarkibini aniqlash zarurligini ko‘rsatadi. Shu bilan birga,

asarda elektron dalillarni amaliy yig‘ish masalalari nisbatan cheklangan doirada yoritilgan [2].

S. W. Brenner «Cybercrime: Criminal Threats from Cyberspace» (2010) asarida kiberjinoyatchilikning tarixiy shakllanishi, uyushgan va transchegaraviy tus olishi hamda huquqni muhofaza qilish organlari uchun yuzaga keladigan qiyinchiliklarni tahlil qilib, hududiy bog‘liqlik zaiflashgan sharoitda tergov yurisdiksiyasi va xalqaro hamkorlik muammolari kuchayishini ochib beradi. Biroq transchegaraviylik har bir kiberjinoyatning zaruriy belgisi emas, shu sababli uni universal ta’rif emas, muayyan ishda tekshiriladigan holat sifatida baholash maqsadga muvofiq [14].

C. D. Ram Clough asariga bag‘ishlangan ilmiy taqrizida (2016) kiberjinoyatlarni «cyber-dependent», «cyber-enabled» va «computer-supported» guruhlarga ajratishning tushunchaviy ahamiyatini ko‘rsatish bilan birga, texnik xavfsizlik, tergov usullari va xalqaro muammolarni yoritish chegaralarini ham qayd etadi. Bu mulohaza jinoyat-huquqiy tasnifni kriminalistik va protsessual tahlil bilan to‘ldirish zarurligini ko‘rsatadi [15].

Mazkur qarashlarni qiyoslash shuni ko‘rsatadiki, Wallning kriminologik yondashuvi texnologiya jinoyat miqyosini qanday o‘zgartirishini tushuntiradi, Cloughning doktrinal tahlili jinoyat tarkibi chegaralarini belgilashga xizmat qiladi, Brenner va Ramning ishlari esa yurisdiksiya hamda tadqiqot metodlarining cheklanishlarini ochib beradi. Ushbu maqolada aynan shu yondashuvlar uyg‘unlashtirilib, raqamli texnologiya jinoyatning bevosita obyekti, sodir etish vositasi yoki faqat aloqa muhiti sifatida ishtirok etishini ajratishga asoslangan tahliliy mezon taklif etiladi.

Tadqiqot normativ-huquqiy hujjatlar va ochiq sud qarorlarini hujjatli tahlil qilishga asoslangan. Tizimli-huquqiy metod orqali jinoyatning belgilari, jinoyat sodir etish usuli va jabrlanuvchiga yetkazilgan zarar o‘rtasidagi aloqalar aniqlanadi. Qiyosiy-huquqiy metod milliy qonunchilikdagi yondashuvni Budapesht konvensiyasi va BMTning Kiberjinoyatlarga qarshi konvensiyasi bilan solishtirish uchun, keys-tahlil esa O‘zbekistondagi birinchi instansiya sud hukmini hamda AQSh sudlarining ikki qarorini huquqiy mantiq nuqtayi nazaridan o‘rganish uchun qo‘llanadi. Normativ bazani O‘zbekiston Respublikasi Jinoyat kodeksi, «Kiberxavfsizlik to‘g‘risida»gi Qonun va ko‘rsatilgan xalqaro hujjatlar tashkil etadi [5, 6, 11, 12]. Xorijiy sud qarorlari milliy huquqning bevosita manbasi sifatida emas, jinoyat tarkibi chegaralarini tahlil qilishga xizmat qiluvchi qiyosiy material sifatida baholandi.

NATIJALAR

Kiberjinoyat tushunchasini internet orqali sodir etilgan barcha huquqbuzarliklar bilan tenglashtirish ilmiy jihatdan aniqlik bermaydi. Zamonaviy tasnifda «cyber-dependent», ya’ni kompyuter tizimiga bevosita bog‘liq jinoyatlar va «cyber-enabled», ya’ni axborot texnologiyasi mavjud jinoyatning ko‘lami, tezligi yoki usulini o‘zgartiradigan jinoyatlar

farqlanadi [4]. Birinchi guruhga ruxsatsiz tizimga kirish, zararli dastur bilan axborotni buzish va xizmat ko‘rsatishga to‘sqinlik qilish, ikkinchi guruhga esa internet-do‘kon orqali aldash, messenjerda yolg‘on va’da berish yoki raqamli to‘lovni suiiste’mol qilish kabi holatlar kiradi.

Mazkur ajratishning huquqiy oqibati katta. Tizimni buzish qilmishida kompyuter ma’lumoti va tarmoqning maxfiyligi, yaxlitligi yoxud mavjudligi bevosita tajovuz obyektidir. Onlayn firibgarlikda esa ko‘pincha asosiy obyekt mulkiy munosabatlar bo‘lib qoladi, raqamli xizmat jinoyatni sodir etish muhiti yoki vositasini tashkil etadi. Shuning uchun «kiber» atamasi kriminologik tasnifda keng, jinoyat tarkibini belgilashda esa qonun matniga bog‘langan torroq ma’noda ishlatiladi [2].

An’anaviy o‘g‘rilikda jinoyat sodir etilgan joy, aybdor va mulk o‘rtasidagi aloqani aniqlash ko‘pincha osonroq. Kiberhujumda esa zararli xabar bir davlatdan jo‘natilib, boshqa yurisdiksiyadagi server orqali o‘tishi va uchinchi davlatdagi bank hisobvarag‘iga ta’sir qilishi mumkin. Hujum boshlangan joy, natija yuz bergan joy, dalil saqlangan joy va jabrlanuvchi yashaydigan hududning mos kelmasligi tergovga tegishlilik, yurisdiksiya, xalqaro so‘rov va dalilni olish muddatini murakkablashtiradi. Shu bilan birga, an’anaviy jinoyat ham har doim jinoyatchi va jabrlanuvchining bevosita uchrashuvini talab qilmaydi: telefon orqali aldash yoki vositachi yordamida sodir etilgan qilmish ham masofaviy bo‘lishi mumkin. Demak, masofa mustaqil va mutlaq tasnif mezoni emas; hal qiluvchi jihat raqamli texnologiyaning jinoyat tarkibidagi vazifasidir.

Jinoyatning tashkiliy modeli ham o‘zgaradi. Zararli dastur ishlab chiquvchi, fishing sahifasini sotuvchi, noqonuniy mablag‘ni boshqa hisobga o‘tkazuvchi va hujumni bevosita amalga oshiruvchi shaxslar turli rollarda harakat qilishi mumkin. Bunda kim muallif, kim tashkilotchi va kim yordamchi ekani faqat texnik izga qarab emas, har bir ishtirokchining bilimi, qasdi, kelishuvi va faktik harakati asosida aniqlanishi kerak. Anonimlashtirish vositasidan foydalanishning o‘zi ham jinoyat niyatini isbotlamaydi: VPN va shifrlash qonuniy maxfiylik maqsadlarida ham qo‘llanadi.

Raqamli zarar faqat bank hisobvarag‘idagi yo‘qotish emas: shaxsiy ma’lumotlar oshkor bo‘lishi, tijorat siri tarqalishi, xizmat ko‘rsatish to‘xtashi va tashkilot obro‘siga putur yetishi ham oqibat bo‘lishi mumkin. Fayl nusxasi bir nechta manzilga tarqalganida u ashyoviy buyum singari asl egasidan butunlay chiqib ketmasa-da, maxfiylik baribir buziladi. Shu sababli an’anaviy «mulk yo‘qoldi – zarar yuz berdi» modeli ma’lumotlar bilan bog‘liq barcha tajovuzlarni tushuntirib bera olmaydi; axborotning maxfiyligi, yaxlitligi va mavjudligi mustaqil muhofaza manfaatlari sifatida ajratilishi zarur [4, 11].

An’anaviy tergovda barmoq izi, qurol yoki voqea joyidagi izlar muhim bo‘lsa, kiberjinoyatda server loglari, tranzaksiya qaydlari, messenjer yozishmalari, fayl metama’lumotlari va qurilma xotirasidagi ma’lumotlar ustuvor dalil bo‘lishi mumkin. Lekin

«elektron dalil har doim tez yo‘qoladi, moddiy dalil esa barqaror» degan qarama-qarshilik ham yetarli emas: har ikkisi buzilishi mumkin. Elektron dalilning xususiyati uning tez nusxalanishi, masofadan o‘zgartirilishi va saqlash muddati xizmat ko‘rsatuvchi siyosatiga bog‘liqligidadir. Shu bois dalil olingan manba, vaqt, yaxlitlikni tekshirish usuli hamda saqlash va topshirish zanjiri hujjatlashtirilishi muhim.

Elektron yozishmaning skrinshoti ayrim faktni ko‘rsatishi mumkin, ammo suhbatning to‘liq konteksti, akkauntning haqiqiy egasi yoki xabar o‘zgartirilmaganini yakka o‘zi isbotlamaydi. Server logining vaqt zonasi, foydalanuvchi identifikatori va IP-manzil kabi ma’lumotlar ham boshqa dalillar bilan tekshirilishi lozim. Budapesht konvensiyasining 16-moddasidagi elektron ma’lumotni tezkor saqlab qolish modeli aynan dalilning yo‘qolish xavfini kamaytirishga qaratilgan [11]. Shu bilan birga, har qanday qidiruv yoki ma’lumot talab qilish protsessual asos, zarurat va mutanosiblik bilan cheklanishi kerak. Olingan natijalar 1-jadvalda umumlashtirilgan.

1-jadval.

An’anaviy jinoyat va kiberjinoyatning qiyosiy tavsifi

Mezon	**An’anaviy jinoyat**	**Kiberjinoyatning o‘ziga xos jihati**
Tajovuz obyekti	Mulk, shaxs, jamoat xavfsizligi va boshqa huquqiy manfaatlar	Axborotning maxfiyligi, yaxlitligi, mavjudligi ham bevosita obyekt bo‘lishi mumkin
Sodir etish vositasi	Jismoniy harakat, hujjat, aloqa yoki boshqa vositalar	Dasturiy kod, hisob qaydnomasi, tarmoq, soxta raqamli interfeys
Makon va yurisdiksiya	Ko‘pincha hodisa joyini aniqlash nisbatan sodda	Ishtirokchi, server va zarar bir necha davlat bilan bog‘lanishi mumkin
Dalillar	Ashyoviy izlar, guvoh ko‘rsatmasi, hujjatlar	Loglar, metama’lumotlar, tranzaksiyalar; autentiklik va saqlash zanjiri muhim
Ko‘lam va takrorlanish	Jismoniy imkoniyat va tashkiliy resurslar bilan cheklanishi mumkin	Avtomatlashtirish orqali ko‘p jabrlanuvchiga bir vaqtning o‘zida ta’sir

Mezon	An’anaviy jinoyat	Kiberjinoyatning o‘ziga xos jihati
Huquqiy kvalifikatsiya	Tarkibning obyektiv va subyektiv belgilariga tayanadi	Raqamli vosita ishlatilgani o‘zi alohida tarkibni isbotlamaydi

MUHOKAMA

O‘zbekiston Respublikasi Jinoyat kodeksida an’anaviy mulkiy jinoyat tarkiblari bilan axborot texnologiyalari sohasidagi maxsus tarkiblar birga amal qiladi [5]. Jumladan, 168-modda firibgarlikni belgilaydi; uning uchinchi qismi «v» bandida axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan firibgarlik alohida ko‘rsatilgan. Bu band 2026-yil 22-iyundagi O‘RQ–1155-sonli qonundan keyingi tahrirda «v» harfi bilan ifodalangan, avvalgi sud hujjatlarida uchraydigan «g» bandi esa o‘sha davrdagi qonun tahriri bilan izohlanadi. Qilmish sodir etilgan va qaror qabul qilingan davrdagi norma hamda hozirgi tahrir o‘rtasidagi farqni ko‘rsatish xatolarning oldini oladi.

Kodeksning XX¹ bobidagi 278¹–278⁹-moddalar axborotlashtirish qoidalarini buzish, kompyuter axborotidan ruxsatsiz foydalanish, maxsus vositalarni tayyorlash yoki tarqatish, kompyuter axborotini modifikatsiyalash, kompyuter sabotaji, zarar keltiruvchi dasturlar, telekommunikatsiya tarmog‘idan noqonuniy foydalanish, kripto-aktivlar aylanmasi va mayning bilan bog‘liq qilmishlarni qamrab oladi. Ularning mavjudligi barcha onlayn aldovlarga shu bobni qo‘llash kerakligini anglatmaydi: tergovchi jinoyat obyektini, amaliy harakatni, oqibatni va qonunda nazarda tutilgan boshqa belgilarni aniq tekshirishi lozim. Mulkiy tajovuz va kompyuter tizimiga tajovuz o‘zaro bog‘langan vaziyatlarda kvalifikatsiya takroriy jazolashga yo‘l qo‘ymasdan, har bir tarkibning mustaqil belgilariga tayanishi kerak.

«Kiberxavfsizlik to‘g‘risida»gi 2022-yilgi O‘RQ–764-son Qonun esa boshqa vazifani bajaradi: u kiberxavfsizlikka oid tashkiliy munosabatlarni, vakolatli davlat organini, muhim axborot infratuzilmasi va hodisalarga javob berish sohasini tartibga soladi [6]. Ushbu Qonun Jinoyat kodeksining o‘rniga o‘tmaydi va har bir kiberhodisani jinoyat deb e’lon qilmaydi. Xavfsizlik hodisasi, texnik zaiflik, intizomiy buzilish, fuqarolik-huquqiy nizo va jinoyat huquqiy tabiati va oqibatlariga ko‘ra farqlanishi kerak.

Jinoyat ishlari bo‘yicha Vobkent tuman sudining 2026-yil 15-maydagi 1-2005-2601/67-sonli hukmida A. Xakimjonov tomonidan Telegram orqali ishontirish va va’da berish asosida jabrlanuvchidan 26,4 million so‘m olingani baholangan [8]. Sud dastlabki tergov qo‘ygan Jinoyat kodeksi 168-moddasi uchinchi qismi «g» bandi (o‘sha paytdagi tahrir) bo‘yicha kvalifikatsiya yetarli darajada isbotlanmagan, degan xulosaga

kelgan, chunki pul o‘tkazilishiga axborot tizimidagi ma’lumotni manipulyatsiya qilish emas, balki jabrlanuvchining shaxsiy ishonchi va ixtiyoriy to‘lovi sabab bo‘lgan. Natijada sud Oliy sud Plenumining 2023-yil 23-iyundagi 17-son qarorining 22-bandiga ham tayanib, qilmishni 168-moddaning birinchi qismi bo‘yicha qayta kvalifikatsiya qilgan.

Mazkur sud hujjati ikkita muhim huquqiy natijani ochib beradi. Birinchidan, messenjer yoki bank kartasining ishtiroki jinoyatning raqamli vositalar yordamida sodir etilgan og‘irlashtirilgan shaklini o‘z-o‘zidan tasdiqlamaydi. Ikkinchidan, «axborot tizimidan foydalanish» belgisini qo‘llash uchun shunchaki telefon orqali muloqot bo‘lganini emas, normaning tarkibiy belgilariga javob beruvchi harakatni va uning dalillarini ko‘rsatish talab qilinadi. Biroq birinchi instansiya hukmidagi xulosa konkret ish dalillariga bog‘liq.

United States v. Morris ishida AQSh Ikkinchi okrug apellyatsiya sudi 1991-yilda kompyuter tarmog‘ida tarqaluvchi «qurt» dasturini ishga tushirish bilan bog‘liq ayblov hukmini kuchda qoldirgan [9]. Sud hujumning ruxsatsiz kirish xususiyatini va o‘sha vaqtdagi Computer Fraud and Abuse Act doirasida aybning zarur subyektiv belgilarini tahlil qilgan. Bu ishda axborot tizimi shunchaki aloqa kanali emas, bevosita ta’sir ko‘rsatilgan muhofaza obyektidir: hujumning texnik mexanizmi kompyuterlarning ishlash qobiliyatiga zarar yetkazgan.

Van Buren v. United States ishida esa AQSh Oliy sudi 2021-yil 3-iyunda vakolatli foydalanuvchining o‘zi kirishi mumkin bo‘lgan ma’lumotni noto‘g‘ri maqsadda olishi har doim ham «ruxsat doirasidan tashqariga chiqish» deb talqin qilinmasligini belgilagan [10]. Sud bu tushunchani foydalanuvchi uchun yopiq bo‘lgan fayl, papka yoki ma’lumotlar bazasi qismlariga kirish bilan bog‘lab, quyi instansiya xulosasini bekor qilgan. Bu ruxsatsiz kirish, xizmat qoidalarini buzish va axloqan nomaqbul xatti-harakatlar o‘rtasidagi chegarani aniq belgilash zarurligini ko‘rsatadi. AQSh huquqidagi bu talqin O‘zbekiston uchun majburiy emas, lekin jinoyat qonunini kengaytirib talqin qilmaslik bo‘yicha qiyosiy dalil bo‘la oladi.

Ko‘rib chiqilgan sud qarorlarida umumiy metodologik talab kuzatiladi: texnologiyadan foydalanish fakti jinoyat tarkibining barcha belgilarini avtomatik ravishda tasdiqlamaydi. Morris ishida axborot tizimiga noqonuniy ta’sir, Van Buren ishida ruxsat chegarasi, Vobkent sudida esa firibgarlik usulining qonundagi maxsus belgiga muvofiqligi muhokama qilingan. Qarorlar turli huquq tizimlariga mansub bo‘lgani bois ularning huquqiy kuchi tenglashtirilmaydi.

BMT Bosh Assambleyasi 2024-yil 24-dekabrda 79/243-rezolyutsiya orqali Kiberjinoyatlarga qarshi konvensiyani qabul qilgan, hujjat 2025-yil 25–26-oktabrda Xanoyda imzolash uchun ochilgan [12]. BMT lozimnomalar reyestriga ko‘ra, O‘zbekiston uni 2025-yil 25-oktabrda imzolagan, ammo 2026-yil 15-noyabr holatida reyestrda O‘zbekistonning ratifikatsiyasi qayd etilmagan; konvensiya ushbu sanada hali kuchga kirmagan [13]. Demak,

imzo qo‘yishni hujjatning kuchga kirishi bilan tenglashtirish noto‘g‘ri; bu lozimnomaning qabul qilinishi, imzolanishi, ratifikatsiyasi va kuchga kirishi bosqichlarini farqlash muhimligini ko‘rsatadi.

Xalqaro hamkorlik boshqa davlatdagi provayderdan abonent ma’lumotini olish, zararli infratuzilmani to‘xtatish va elektron izlarni saqlab qolish uchun zarur. Lekin bu ehtiyoj cheklanmagan kuzatuvga asos bo‘la olmaydi. Elektron yozishmalarni oshkor qilish, qurilmani tintuv qilish va chet eldan ma’lumot talab etish qonuniy asos, zarurat, mustaqil nazorat va shaxsiy hayot daxlsizligi bilan muvozanatlantirilishi lozim, aks holda kiberjinoyatchilikka qarshi siyosatning o‘zi raqamli huquqlarga ortiqcha aralashuvga sabab bo‘lishi mumkin.

Bir yondashuv texnologiyaning tezligi, ommaviyligi, transchegaraviyligi va anonimlashtirish imkoniyatlarini yuqori ijtimoiy xavflilik belgisi deb baholaydi: phishing orqali minglab shaxsga murojaat qilish oddiy bir martalik aldovdan kengroq oqibat keltirishi mumkin. Boshqa yondashuv esa faqat raqamli vositadan foydalanilgani uchun har bir qilmishga og‘irroq javobgarlik yuklash huquqiy aniqlik va mutanosiblikni buzishi mumkinligini ko‘rsatadi: messenjerda oddiy yolg‘on va’da bergan shaxsni tizimga kirib ma’lumotni o‘zgartirgan hujumchi bilan bir xil baholab bo‘lmaydi.

Tadqiqot pozitsiyasiga ko‘ra, ikki yondashuvni birlashtiruvchi mezon – raqamli texnologiya aynan qanday qo‘shimcha xavf tug‘dirganini isbotlashdir. Axborot tizimini aldash yoki buzish, avtomatlashtirilgan ommaviy hujum, katta ko‘lamdagi zarar, muhim infratuzilmaga ta’sir yoki xavfsizlik mexanizmlarini chetlab o‘tish texnologiyaning mustaqil kriminogen ahamiyatini ko‘rsatishi mumkin, oddiy onlayn muloqotning o‘zi esa bunday xulosaga olib kelmaydi. Bunda ayni holat bir necha marta og‘irlashtiruvchi omil sifatida hisoblanmasligi kerak.

Tadqiqot natijalaridan kelib chiqib, quyidagi amaliy takliflar ilgari suriladi. Birinchidan, elektron dalillarga ishlov berishning yagona amaliy standartlarini kuchaytirish: log va yozishmalarni tezkor saqlash, ularning kelib chiqishini qayd etish, tekshiruv uchun olingan nusxaning yaxlitligini hujjatlashtirish, ekspert xulosasini boshqa dalillar bilan solishtirish hamda himoya tomoniga dalillarni tekshirish imkonini berish.

Ikkinchidan, banklar, to‘lov tashkilotlari, aloqa operatorlari va vakolatli organlar o‘rtasida qonuniy asosga ega tezkor xabar berish va firibgarlikni to‘xtatish mexanizmlarini kengaytirish. Shubhali tranzaksiyani erta aniqlash jabrlanuvchi zararini kamaytiradi, biroq ma’lumot almashish doirasi aniq belgilanishi va shaxsiy axborotning ortiqcha yig‘ilishiga yo‘l qo‘yilmasligi lozim.

Uchinchidan, profilaktikani faqat foydalanuvchining ehtiyotsizligiga bog‘lamaslik. Raqamli savodxonlik bilan bir qatorda bank va platformalarga xavfsiz identifikatsiya, shubhali harakatlarni aniqlash, ma’lumotlarni minimal yig‘ish va hodisaga javob berish

majburiyatlarini amalda bajarish bo‘yicha talablar qo‘yilishi kerak, chunki zamonaviy kiberjinoyat muvaffaqiyatiga nafaqat insonning ishonuvchanligi, balki tizimning dizayni va tashkiliy kamchiliklar ham ta’sir ko‘rsatadi.

XULOSA

Tahlil kiberjinoyatlarning an’anaviy jinoyatlardan farqi yagona texnik belgida emas, bir nechta omilning uyg‘unligida namoyon bo‘lishini ko‘rsatdi. Bular – kompyuter tizimining ba’zan tajovuzning mustaqil obyektiga aylanishi, avtomatlashtirish hisobiga ko‘lamning kengayishi, bir nechta yurisdiksiyaning tutashuvi, raqamli dalillarni saqlashning maxsus talablari, yangi ishtirokchilik modellari hamda maxfiylik va tizim mavjudligiga zarar yetkazish imkoniyatidir. Shu bilan birga, kiberjinoyat an’anaviy jinoyatdan mutlaqo ajralgan mustaqil dunyo emas: onlayn firibgarlikda aldash va o‘zgalar mulkini egallash kabi asosiy jinoiy-huquqiy belgilar saqlanib qolishi mumkin.

Milliy qonunchilik maxsus kompyuter jinoyatlarini ham, axborot texnologiyalari vositasida sodir etilgan ayrim an’anaviy jinoyatlarning kvalifikatsiyalangan tarkiblarini ham nazarda tutadi. Vobkent sudi hukmi, Morris va Van Buren ishlari texnologik shaklning o‘zini jinoyat tarkibi bilan adashtirmaslik zarurligini tasdiqlaydi. Qonuniylik va aybsizlik prezumpsiyasi qilmishning texnik usulini, ayblanuvchining vakolati doirasini va zararli oqibatni ishonchli dalillar bilan asoslashni talab qiladi.

Tadqiqot natijalariga ko‘ra, kiberjinoyatchilikka qarshi huquqiy siyosatning samaradorligi jazoni umumiy ravishda og‘irlashtirishdan ko‘ra, jinoyat tarkibini aniq belgilash, elektron dalillarni ishonchli tekshirish, xalqaro protsessual hamkorlikni rivojlantirish va shaxs huquqlarini kafolatlashning o‘zaro uyg‘unligiga bog‘liq. Texnologik yangilanishlar huquqiy normalarni takomillashtirishni talab etadi, biroq qonuniylik prinsipi jinoyat tarkibini analogiya yoki kengaytiruvchi talqin orqali sun’iy ravishda shakllantirishga yo‘l qo‘ymaydi.

FOYDALANILGAN ADABIYOTLAR

1. Yar, M. Cybercrime and Society. – SAGE Publications, 2006.
2. Clough, J. Principles of Cybercrime. 2nd ed. – Cambridge University Press, 2015. – ISBN 9781107034570.
3. Wall, D. S. Cybercrime: The Transformation of Crime in the Information Age. – Polity Press, 2007.
4. Council of Europe. Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence. – https://rm.coe.int/3148-3-1-12-guide-for-criminal-justice-statistics-on-cybercrime-and-ee/1680a0250a

5. O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil 22-sentabr; 2026-yil 15-oktabrdagi tahrir). 168 va 278¹–278⁹-moddalar. – https://lex.uz/uz/docs/-111453

6. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni, 2022-yil 15-aprel, O‘RQ–764. – https://www.lex.uz/mact/-5960604

7. O‘zbekiston Respublikasi Ichki ishlar vazirligi. «Kiberjinoyatlarni jilovlash orqali xavfsiz kibermakon yaratish», 2025. – https://gov.uz/oz/iiv/news/view/52319

8. Jinoyat ishlari bo‘yicha Vobkent tuman sudining 2026-yil 15-maydagi hukmi, ish № 1-2005-2601/67. – https://publication.sud.uz/api/file/criminal/3121457

9. United States v. Morris, 928 F.2d 504 (2nd Cir., March 7, 1991). – https://law.justia.com/cases/federal/appellate-courts/F2/928/504/452673/

10. Van Buren v. United States, 593 U.S. 374 (June 3, 2021). – https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf

11. Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No. 185, 23 November 2001. – https://www.refworld.org/legal/agreements/coe/2001/90189

12. United Nations General Assembly. Resolution 79/243 and annex: United Nations Convention against Cybercrime, 24 December 2024. – https://mandates.un.org/mandate/A/RES/79/243

13. United Nations Treaty Collection. United Nations Convention against Cybercrime: Status of signatures, ratifications and entry into force (15 November 2026 holatiga). – https://treaties.un.org

14. Brenner, S. W. Cybercrime: Criminal Threats from Cyberspace. – Praeger, 2010.

15. Ram, C. D. Book Review: Jonathan Clough, Principles of Cybercrime, 2nd ed. // Canadian Journal of Law and Technology. – 2016. – Vol. 14, No. 1.