AXBOROT TEXNOLOGIYALARI SOHASIDAGI JINOYATLARNI ANIQLASHDA XALQARO-HUQUQIY YORDAM VA TEZKOR AXBOROT ALMASHINUVI

Mirzaabdullayev Shoxrux Otajon o‘g‘li
(O‘zbekiston Respublikasi IIV Akademiyasi kursanti)
Iminov Abdurasul Abdulatipovich
(O‘zbekiston Respublikasi IIV Akademiyasi
Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig‘i)

Annotatsiya: Ushbu maqolada axborot texnologiyalari sohasidagi jinoyatlarni (kiberjinoyatlarni) aniqlash, tergov qilish va ularning oldini olishda transmilliy hamkorlik, xalqaro-huquqiy yordam hamda tezkor axborot almashinuvi mexanizmlarining huquqiy va amaliy asoslari tahlil qilinadi. Kibermakonning chegarasiz tabiati va raqamli dalillarning o‘ta o‘zgaruvchanligi (volatile nature) sharoitida an’anaviy huquqiy yordam ko‘rsatish usullarining samaradorligi pastligi asoslab berilgan. Tadqiqotda kiberjinoyatchilikka qarshi kurashishda xalqaro konvensiyalar (jumladan, Budapesht konvensiyasi), Interpol, Yevropol kabi tashkilotlarning roli hamda "24/7" tezkor aloqa tarmoqlarining ahamiyati yoritilgan. Maqola yakunida milliy qonunchilikni xalqaro standartlar bilan uyg‘unlashtirish va davlatlararo real vaqt rejimidagi (real-time) ma’lumot almashinuvini optimallashtirish bo‘yicha takliflar ilgari surilgan.

Kalit so‘zlar: kiberjinoyatchilik, xalqaro-huquqiy yordam, tezkor axborot almashinuvi, raqamli dalillar, transmilliy jinoyatlar, Budapesht konvensiyasi, Interpol, 24/7 aloqa tarmog‘i, kiberxavfsizlik, huquqiy hamkorlik, yurisdiksiya, ekstraditsiya.

Abstract: This article analyzes the legal and practical foundations of transnational cooperation, mutual legal assistance, and rapid information exchange mechanisms in detecting, investigating, and preventing crimes in the field of information technology (cybercrimes). It substantiates that traditional methods of legal assistance are inefficient given the borderless nature of cyberspace and the highly volatile nature of digital evidence.

The study highlights the role of international conventions (including the Budapest Convention), organizations such as Interpol and Europol, and the significance of "24/7" emergency communication networks in combating cybercrime. The article concludes with proposals directed at harmonizing national legislation with international standards and optimizing real-time data exchange between states.

Keywords: cybercrime, mutual legal assistance, rapid information exchange, digital evidence, transnational crimes, Budapest Convention, Interpol, 24/7 network, cybersecurity, legal cooperation, jurisdiction, extradition.

Аннотация: В данной статье анализируются правовые и практические основы транснационального сотрудничества, международно-правовой помощи и механизмов оперативного обмена информацией в сфере выявления, расследования и предупреждения преступлений в области информационных технологий (киберпреступлений). Обосновано, что традиционные методы оказания правовой помощи малоэффективны в условиях трансграничного характера киберпространства и высокой изменчивости (летучести) цифровых доказательств. В исследовании освещаются роль международных конвенций (включая Будапештскую конвенцию), деятельность таких организаций, как Интерпол и Европол, а также значение сетей оперативной связи "24/7" в борьбе с киберпреступностью. В заключении статьи выдвинуты предложения по гармонизации национального законодательства с международными стандартами и оптимизации межгосударственного обмена данными в режиме реального времени.

Ключевые слова: киберпреступность, международно-правовая помощь, оперативный обмен информацией, цифровые доказательства, транснациональные преступления, Будапештская конвенция, Интерпол, сеть 24/7, кибербезопасность, правовое сотрудничество, юрисдикция, экстрадиция.

Kiberjinoyatlarning 90% dan ortig‘i transchegaraviy (transnational) xarakterga ega. Ya’ni, jinoyat sodir etilgan joy, yetkazilgan zarar va raqamli dalillar (IP-manzillar, log-fayllar, kriptovalyuta hamyonlari) dunyoning turli chekkalarida joylashgan bo‘ladi. O‘zbekiston yurisdiksiyasida ushbu muammolarni hal qilish uchun bir nechta huquqiy

platformalar va yangilangan mexanizmlar mavjud. Bularga Budapesht konvensiyasi prinsiplari, ikki tomonlama shartnomalar (MLAT) hamda O‘zbekiston Respublikasi Kiberxavfsizlik markazi DUK va IIV Kiberjinoyatchilikka qarshi kurashish boshqarmasining xalqaro CERT tarmoqlari hamda Interpol bilan to‘g‘ridan-to‘g‘ri aloqa kanallari kiradi. Masalan, O‘zbekistondagi e-commerce saytining to‘lov tizimi Germaniyadagi server orqali xakerlar tomonidan buzib kirilgan bo‘lsa, O‘zbekiston huquq-tartibot idoralari Germaniya hukumatiga raqamli dalillarni muzlatib qo‘yish (preservation of data) bo‘yicha rasmiy va tezkor so‘rov yuborishi mumkin.

Ko‘plab IT kompaniyalar va startaplar xalqaro huquqiy mexanizmlarni tushunmasliklari sababli kiberhujum paytida eng muhim dalillarni yo‘qotib qo‘yadilar. Birinchidan, raqamli dalillar noto‘g‘ri saqlanadi va Chain of Custody qoidasi buziladi. Hujumga uchragan server log-fayllarini shunchaki skrinshot qilib olish huquqiy kuchga ega emas. Xalqaro sudda yoki xorijiy provayderga so‘rov yuborishda dalillar xalqaro standartlarga (masalan, ISO/IEC 27037) muvofiq, xesh-qiymatlari (hash values) bilan muhrlanishi kerak. Ikkinchidan, yurisdiksiya konflikti hisobga olinmaydi. Agar serveringiz ma’lumotlar maxfiyligini o‘ta qattiq himoya qiladigan (masalan, Shveysariya yoki Islandiya) davlatda bo‘lsa, u yerdan tezkor ma’lumot olish va xalqaro so‘rov o‘tkazish juda murakkab kechadi. Uchinchidan, vaqt boy beriladi. Kiberjinoyatda raqamli izlar juda tez o‘chib ketadi. Provayderlar log-fayllarni odatda 30 tadan 90 kungacha saqlaydi, xalqaro rasmiy so‘rov (MLA) yuborish va uning tasdiqlanishi esa oylarni talab qilishi mumkin.

Agar kompaniyangiz xalqaro kiberjinoyat qurboniga aylansa yoki buni oldindan sug‘urtalashni istasangiz, tizimli qadamlarni amalga oshirishingiz shart. Avvalo, raqamli dalillarni "muzlatish" (Data Preservation) lozim. Ichki xavfsizlik xizmati orqali hujum sodir bo‘lgan tizimlarning "snapshot" (nusxa)sini oling va loglarni o‘zgartirib bo‘lmaydigan formatda saqlang. Keyingi bosqichda "24/7 Aloqa Nuqtalari" (Points of Contact) bilan bog‘laning. O‘zbekiston Respublikasi Huquq-tartibot organlari (Kiberxavfsizlik markazi yoki IIV) orqali Interpolning 24/7 kiberxavfsizlik tarmog‘idan foydalaning. Bu rasmiy tergov to‘liq boshlanguncha xorijiy provayderdagi ma’lumotlarni o‘chib ketishidan vaqtincha saqlaydi. Shuningdek, bulutli provayderlarning (AWS, Azure,

DigitalOcean) maxsus orderlarini ishga tushiring. Agar jinoyatchi yirik global platformalardan foydalangan bo‘lsa, advokatingiz orqali ushbu kompaniyalarning "Emergency Disclosure Request" (Favqulodda ma’lumot taqdim etish so‘rovi) tizimiga ariza bering. Yakunda esa zararni baholash va Sud-IT Ekspertizasini o‘tkazing. O‘zbekiston Jinoyat Kodeksining 278-moddalari (Axborot texnologiyalari sohasidagi jinoyatlar) bo‘yicha jinoiy ish ochish va xalqaro yordam so‘rash uchun aynan qaysi tizimga noqonuniy kirilgani va moddiy zarar miqdori rasmiy ekspertiza orqali aniq hisoblanishi shart.

Xulosa o‘rnida aytish mumkinki, kiberjinoyatchilik — bu shunchaki texnik muammo emas, bu global huquqiy kurash maydonidir. O‘zbekistondagi IT loyihalar xalqaro bozorda xavfsiz rivojlanishi uchun nafaqat kuchli Senior dasturchilarga, balki xalqaro huquqiy yordam va tezkor axborot almashinuvi mexanizmlarini tushunadigan Cyber Lawyer (Kiber-huquqshunos) ko‘magiga ham muhtoj. Biznesingiz raqamli infratuzilmasini xalqaro huquq normalariga moslashtiring, xavfsizlik loglarini to‘g‘ri yuriting va kiber-tahdidlarga har doim huquqiy jihatdan tayyor turing. Biznesingiz xavfsizligi — sizning eng katta aktivingizdir!

Raqamli infratuzilmaning xalqaro huquq normalariga muvofiqligini ta’minlash va kiber-tahdidlarga huquqiy jihatdan shay turish strategiyasi, aslida, xalqaro-huquqiy yordam institutining eng murakkab mexanizmlarini va ularning amaliy ishlash prinsiplarini chuqur tahlil qilishni taqozo etadi. Amaliyotda ko‘plab transmilliy kiberjinoyatlarni tergov qilish jarayoni aynan davlatlararo huquqiy munosabatlarning tabiati sababli murakkablashadi. Xalqaro-huquqiy yordam (MLA) mexanizmi o‘z mohiyatiga ko‘ra suveren davlatlarning o‘zaro shartnomaviy majburiyatlariga tayanadi. Agar kiberhujum uyushtirgan xaker joylashgan davlat bilan O‘zbekiston o‘rtasida ikki tomonlama huquqiy yordam ko‘rsatish to‘g‘risidagi shartnoma (MLAT) mavjud bo‘lmasa, jarayon xalqaro huquqdagi "o‘zaro manfaatdorlik va hurmat" (comity) prinsipiga ko‘ra amalga oshiriladi, bu esa protsessual vaqtni ikki barobarga uzaytirib yuboradi. Kiberjinoyat sodir etilganda dastlabki 48 soat ichida raqamli dalillarni saqlab qolish va jinoyatchining virtual izini yo‘qotmaslik uchun an’anaviy MLA diplomatik kanallaridan

foydalanish ko‘pincha kutilgan natijani bermaydi. Shuning uchun zamonaviy xalqaro kiberhuquqda diplomatik so‘rovlar o‘rnini operativ va tezkor axborot almashish tarmoqlari egallamoqda.

Ushbu tezkor axborot almashinuvi tizimining markazida G7 va Evropa Kengashi tomonidan tashkil etilgan hamda Budapesht konvensiyasi bilan qonuniy mustahkamlangan 24/7 doimiy aloqa nuqtalari tarmog‘i (24/7 Network) turadi. Ushbu tarmoqning tashkiliy ustuvorligi shundaki, har bir a’zo davlatda kiberjinoyatlarga qarshi kurashuvchi maxsus vakolatli organ tun-u kun ish rejimida faoliyat yuritadi va boshqa davlatdan kelgan favqulodda so‘rovlarni qabul qilgan hamono rasmiy MLA orderi tayyor bo‘lgunga qadar raqamli ma’lumotlarni o‘chib ketishidan himoya qiladi (Data Preservation order). O‘zbekiston huquq-tartibot idoralari va Kiberxavfsizlik markazlarining ushbu global tezkor tarmoqlar bilan integratsiyalashuvi mahalliy biznes va davlat obyektlarini xorijiy xakerlar hujumidan himoya qilish darajasini tubdan oshirmoqda. Biroq, bu yerda yana bir xalqaro huquqiy muammo — "ikki tomonlama jinoiylik" (double criminality) prinsipi yuzaga keladi. Ya’ni, so‘rov yuborayotgan davlatda (O‘zbekistonda) jinoyat deb hisoblangan qilmish (masalan, Jinoyat Kodeksining 278-moddalaridagi tizimga noqonuniy kirish yoki modifikatsiya qilish), so‘rov borayotgan xorijiy davlat qonunchiligida ham aynan jinoiy javobgarlikka sabab bo‘ladigan qilmish sifatida tan olinishi shart. Agar jinoyatchi o‘tirgan davlat qonunchiligida muayyan turdagi kiber-faoliyat yoki virtual aktivlar manipulyatsiyasi jinoyat deb tasniflanmagan bo‘lsa, u holda xalqaro huquqiy yordam ko‘rsatish rad etilishi mumkin.

Bundan tashqari, transmilliy kiberjinoyatlarni aniqlashda global texnologik gigantlar va bulutli provayderlarning (masalan, Google, Microsoft, Amazon Web Services, Cloudflare) ichki korporativ xavfsizlik siyosati va maxfiylik deklaratsiyalari bilan ishlash alohida huquqiy mahorat talab qiladi. Hozirgi kunda aksariyat xalqaro kiberhujumlar yirik transmilliy IT-kompaniyalarning serverlarida joylashgan infratuzilmalardan tranzit sifatida foydalangan holda amalga oshiriladi. Davlatlararo rasmiy MLA so‘rovlari oylab vaqt olishini inobatga olib, zamonaviy kiber-prokurorlar va kiber-huquqshunoslar to‘g‘ridan-to‘g‘ri ushbu korporatsiyalarning huquqiy departamentlariga Favqulodda

ma’lumotlarni oshkor qilish so‘rovlari (Emergency Disclosure Requests — EDR) bilan murojaat qilish mexanizmidan foydalanmoqdalar. AQShning "Elektron aloqa maxfiyligi to‘g‘risidagi qonuni" (ECPA) va Yevropa Ittifoqining ma’lumotlarni himoya qilish bo‘yicha umumiy reglamenti (GDPR) kabi qattiq qonunchilik hujjatlarida ham, inson hayotiga xavf tug‘ilganda yoki milliy xavfsizlik hamda kritik infratuzilmaga yirik iqtisodiy tahdid mavjud bo‘lganda, xususiy provayderlar rasmiy sud orderisiz ham tezkor ma’lumotlarni (foydalanuvchining login tarixi, IP-manzili, to‘lov ma’lumotlari) huquq-tartibot idoralariga taqdim etish huquqiga egaligi belgilangan.

Xalqaro hamkorlikning yana bir murakkab va yangi yo‘nalishi — virtual aktivlar va kriptovalyutalar bilan bog‘liq kiberjinoyatlarni tergov qilish va ularni xalqaro miqyosda muzlatish amaliyotidir. Bugungi kunda kiberfiribgarlik, onlayn tovlamachilik (ransomware) va noqonuniy hakerlik hujumlari natijasida qo‘lga kiritilgan mablag‘lar deyarli 100% holatlarda kriptovalyuta hamyonlariga o‘tkaziladi. Kiberjinoyatchilar blokcheyn tizimidagi anonimlikdan foydalanib, mablag‘larni yuzlab hamyonlar aro parchalab yuborishadi va markazlashmagan birjalar (DEX) yoki mikser dasturlari orqali izlarni chalkashtirishga urinishadi. Bunday sharoitda jinoyatni aniqlash va mablag‘larni qaytarish uchun "Blokcheyn kriminalistikasi" (Blockchain Forensics) tahlil usullari qo‘llaniladi. FATF (Pul yuvishga qarshi kurashish bo‘yicha xalqaro guruh) standartlariga muvofiq, dunyodagi barcha yirik kriptobirjalar (masalan, Binance, Coinbase) "O‘z mijozingni bil" (KYC) va pul yuvishga qarshi kurashish (AML) qoidalariga rioya qilishga majburdirlar. O‘zbekiston Respublikasi huquq-tartibot organlari xalqaro hamkorlik doirasida hakerlar foydalangan tranzaksiyalarning zanjirini tahlil qilib, mablag‘lar borib tushgan hamyon muayyan xalqaro birjaga tegishli ekanligini aniqlagan lahzada, tezkor axborot almashinuvi kanallari orqali ushbu birja ma’muriyatiga hamyonni bloklash (freeze) bo‘yicha shoshilinch so‘rov yuborishi mumkin. Bu choralar transmilliy kiberjinoyat orqali yetkazilgan iqtisodiy zararni real vaqt rejimida qoplashning eng samarali huquqiy-texnik vositasidir.

Biroq, tizimli tahlillar shuni ko‘rsatadiki, transmilliy darajada kiberjinoyatchilikka qarshi kurashishda global yurisdiksiya kolliziyalari (to‘qnashuvlari) hamon eng yirik

huquqiy muammo bo‘lib qolmoqda. Ba’zi davlatlar o‘z hududidagi xakerlar faoliyatiga geosiyosiy manfaatlar sababli ko‘z yumadilar yoki ularni xalqaro ekstraditsiya qilishdan mutlaqo bosh tortadilar. Ushbu muammoni hal qilish va global raqamli makonda "xavfsiz boshpanalar" (cyber-havens) paydo bo‘lishining oldini olish uchun xalqaro hamjamiyat BMT shafeligida kiberjinoyatchilikka qarshi kurashish to‘g‘risidagi yangi, universal va barcha davlatlar uchun majburiy bo‘lgan Global konvensiyani ishlab chiqish ustida faol ish olib bormoqda. Bunday sharoitda O‘zbekiston Respublikasining milliy qonunchiligi va amaliyoti nafaqat mintaqaviy (MDH, ShHT) miqyosda, balki global miqyosda raqamli dalillar bilan ishlash, elektron so‘rovlarni qabul qilish va yuborish borasida to‘liq texnik va huquqiy moslashuvchanlikka (interoperability) ega bo‘lishi strategik vazifadir.

Xulosa o‘rnida va yakuniy tahlil sifatida ta’kidlash lozimki, axborot texnologiyalari sohasidagi jinoyatlarni muvaffaqiyatli aniqlash va ularga chek qo‘yish — faqatgina bir davlatning ichki texnik imkoniyatlari yoki mudofaa devorlari (firewalls) bilan hal bo‘ladigan masala emas. Kiberjinoyatchilik o‘zining mohiyati va arxitekturasiga ko‘ra chegaralarni tan olmas ekan, unga qarshi kurash ham global, birlashgan va o‘ta tezkor huquqiy xarakterga ega bo‘lishi shart. O‘zbekistonning FinTech ekotizimi va raqamli iqtisodiyoti xalqaro maydonda mustahkam o‘rin egallashi uchun davlat organlari va xususiy biznes o‘rtasida kiber-tahdidlar haqidagi axborotlarni tezkor almashish (cyber threat intelligence sharing) madaniyati shakllanishi, milliy protsessual normalar raqamli dalillarni xalqaro andozalarda muhrlash qobiliyatiga ega bo‘lishi hamda xalqaro huquqiy yordam (MLA) mexanizmlaridan maksimal darajada professional foydalanilishi lozim. Kelajak ruhan va jismonan raqamlashtirilgan dunyoda kechar ekan, kiberxavfsizlik sohasidagi transmilliy va tezkor huquqiy hamkorlik — milliy suverenitetni va iqtisodiy barqarorlikni virtual makonda himoya qilishning eng bosh va fundamental kafolati bo‘lib qolaveradi.

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasi Konstitutsiyasi. – Toshkent, 2023;

2. O‘zbekiston Respublikasi Jinoyat kodeksi. – Toshkent: Adliya vazirligi nashriyoti, 2023;

3. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni (2003 yil 11 dekabr);

4. O‘zbekiston Respublikasi “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni (2019 yil 2 iyul);

5. Ro‘ziyev R.N., Salayev N.S. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar: monografiya. — Toshkent: TDYU, 2018;

6. Anorboyev A.U. Kiberjinoyatlarning jinoiy-huquqiy jihatlari: dissertatsiya. — Toshkent, 2020.