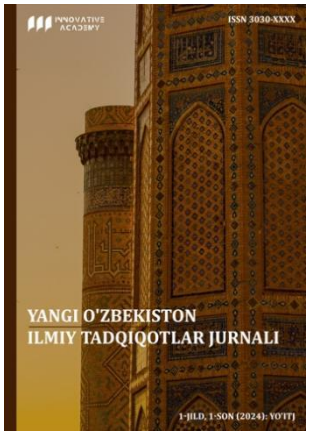

KIBERJINOYATLARGA QARSHI XALQARO KONVENSIYALAR VA MILLIY QONUNCHILIK TAHLILI

To'lqinova Visola Ulug'bek qizi

Toshkent davlat yuridik universiteti

Jinoiy odil sudlov fakulteti talabasi

E-mail: visolatolqinova05@gmail.com

https://doi.org/10.5281/zenodo.20520362

ARTICLE INFO

Qabul qilindi: 11-may 2026 yil
Ma'qullandi: 15-may 2026 yil
Nashr qilindi: 31-may 2026 yil

KEY WORDS

xalqaro konvensiyalar, kiberjinoyatlar, Budapesht konvensiyasi, raqamli huquq, kiberxavfsizlik, milliy qonunchilik, sun'iy intellekt, BMT, ma'muriy javobgarlik, xalqaro hamkorlik.

ABSTRACT

XXI asrda raqamli texnologiyalarning misli ko'rilmagan sur'atlarda rivojlanishi insoniyat hayotini tubdan o'zgartirdi. Biroq bu o'zgarishlar bilan birga yangi turdagi jinoyatchilik jumladan kiberjinoyatlar ham shiddatli tarzda avj olmoqda. Hech bir davlat, tashkilot yoki jismoniy shaxs ushbu tahdiddan mutlaqo himoyalanmagan. Ushbu maqolada kiber huquqning tarixi va konseptual asoslari, kiberjinoyatlar tasnifi hamda ularga qarshi kurashda xalqaro hamkorlikning huquqiy mexanizmlari, xususan, Budapesht konvensiyasi, Palermo konvensiyasi va BMT tomonidan ishlab chiqilayotgan yangi konvensiya loyihasi tahlil qilinadi. O'zbekiston Respublikasining milliy qonunchiligi Jinoyat kodeksi va Ma'muriy javobgarlik to'g'risidagi kodeksi xalqaro standartlar bilan qiyosiy o'rganilib, qonunchilikdagi bo'shliqlar aniqlangan va takliflar berilgan. Shuningdek, Buyuk Britaniya, AQSh va Oksford universiteti tadqiqotlari asosida kiberjinoyatlar statistikasi keltirilgan. Maqola o'zbekistonlik va xorijiy olimlarning ilmiy qarashlari bilan tahlil qilingan bo'lib, muallif o'z taklif va xulosalarini ilmiy asosda ifodalagan.

Kirish

Bugungi globallashuv davrida internet va raqamli texnologiyalar insoniyatning ijtimoiy, iqtisodiy va siyosiy hayotining ajralmas bo'g'iga aylanib bormoqda. 2024-yil holatiga ko'ra dunyo bo'ylab internet foydalanuvchilari soni 5,5 milliard nafardan oshdi[1]. Shu bilan birga raqamli muhit turli turdagi jinoyatlar uchun qulay maydon bo'lmoqda. Kiberjinoyatlar — ya'ni axborot texnologiyalari vositasida sodir etiladigan jinoyatlar hozirgi kunda xalqaro darajada eng tez o'sib borayotgan jinoyat turlaridan biriga aylandi. Jahon iqtisodiy forumi hisobotida qayd etilishicha, uyushgan kiberjinoyat idoralari jinoiy faoliyatni tobora onlayn ko'chirmoqda va ularning aniqlash hamda jinoiy javobgarlikka tortilish ehtimoli AQShda 1 foizdan ham past darajada qolmoqda[2].

Xalqaro huquqshunoslar kiberjinoyatlarning milliy qonunchilik chegarasini kesib o'tuvchi, transchegaraviy xarakter kasb etishini uzoq yillardan beri ta'kidlab kelmoqda. Monash universiteti professori Jonathan Clough o'zining Cambridge University Press tomonidan chop

etilgan asarida kiberjinoyatlarning global tabiati barcha davlatlar uchun qonunchilikni zamonaviy texnologiyalar bilan tenglashtirish muammosini keltirib chiqarayotganini ko'rsatib bergan[3]. Bert-Jaap Koops va Susan Brenner ilmiy izlanishlaridagi qiyosiy tadqiqot esa kiberjinoyatlar bilan kurashda xalqaro tergov va yurisdiktsiya masalalaridagi tizimli bo'shliqlarni batafsil tahlil qilgan[4].

UNODCning keng qamrovli tadqiqotida ta'kidlanganidek[5], xalqaro konvensiyalarning milliy qonunchilikka implementatsiya qilinishi jarayonida huquqiy bo'shliqlar deyarli barcha mintaqalarda, ayniqsa Budapesht konvensiyasiga a'zo bo'lmagan davlatlarda keng tarqalgan. O'zbekiston misolida bu muammoni A.Atkhamjonov ham alohida ta'kidlab, mamlakatning xalqaro standartlarga muvofiq islohotlar yo'liga endigina kirganini qayd etgan[6]. BMTning Giyovand moddalar va jinoyatchilikka qarshi idorasi (UNODC) ning 2013-yilgi keng qamrovli tadqiqotida qayd etilishicha, dunyo bo'yicha javob bergan davlatlarning yarmidan kami o'zlarining jinoiy va protsessual huquq tizimlarini yetarli deb hisoblaydi; Yevropa davlatlarining uchdan ikki qismidan ko'prog'i qonunchiligi yetarli deb baholagan holda, boshqa mintaqalar, jumladan Markaziy Osiyo davlatlari sezilarli darajada orqada qolmoqdaligini ta'kidlaydi[7]. O'zbekiston o'zining Budapesht konvensiyasiga qo'shilish jarayonini rasmiy boshlashini 2025-yilda e'lon qildi, bu esa milliy qonunchilikning xalqaro standartlarga muvofiqlashtirish zarurligi allaqachon tan olinganini ko'rsatadi[7]. Ushbu maqola aynan shu bo'shliqlarni to'ldirishga, mavjud xalqaro konvensiyalarni O'zbekiston milliy qonunchiligida qiyosiy o'rganishga hamda tegishli taklif va xulosalar ishlab chiqishga qaratilgan.

Metodologiya

Ushbu tadqiqot qiyosiy-huquqiy, tarixiy-huquqiy va empirik tahlil metodlari asosida amalga oshirildi. Birinchidan, xalqaro konvensiyalar, jumladan Budapesht konvensiyasi matni, Palermo konvensiyasi va BMT ning kiberjinoyatlar to'g'risidagi konvensiya loyihasi O'zbekiston Respublikasi amaldagi qonunchilik hujjatlari bilan qiyosiy o'rganildi. Ikkinchidan, O'zbekiston Respublikasi my.sud.uz portali orqali kiberjinoyatlarga oid real sud qarorlari va ishlar tahlil qilindi. Uchinchidan, Pew Research Center, Oksford universiteti va Buyuk Britaniya Milliy Statistika Idorasining so'ngi hisobotlari statistik manba sifatida ishlatildi. To'rtinchidan, Jonathan Clough, Koops va Brenner, Jon Bandler, Hai Thanh Luong kabi xorijiy olimlarning ilmiy asarlari tanqidiy tahlil qilindi. Rasmiy xalqaro hujjatlar orasida UNODCning keng qamrovli kiberjinoyatlar tadqiqoti, OSCEning O'zbekiston bo'yicha hisoboti hamda R.R.Shakurov va M.M.Vohidovlarning O'zbekistonlik mutaxassis sifatida tayyorlagan risola asarlari tadqiqotning nazariy asosini tashkil qildi. Kiberjinoyatlarni tahlil qilishda sud-kriminalistika, axborot xavfsizligi va raqamli dalillarni o'rganish metodologiyasidan ham foydalanildi.

MUHOKAMA VA NATIJALAR

Kiber huquq — axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solishga hamda himoya qilishga qaratilgan huquq sohasidir. R.R.Shakurov va M.M.Vohidov rasmiy o'uv qo'llanmasida ta'kidlanganidek, O'zbekistonda raqamli iqtisodiyot rivojlanishi bilan kiberhuquqni mustaqil soha sifatida o'rganish zarurligi tobora ortib bormoqda[8]. Kiber huquqining ildizlari 1960-yillarga borib taqaladi — aynan o'sha davrda kompyuter texnologiyalari rivojlana boshlagan edi. 1970–1980-yillarda shaxsiy kompyuterlar va tarmoqlarning paydo bo'lishi ushbu sohani yanada dolzarb qildi. Cloughning akademik asarida ko'rsatilganidek[9], 1990-yillarning o'rtalaridan boshlab kiber huquq mustaqil huquq tarmog'i sifatida shakillana boshladi va davlatlar buni qonunchilik darajasida tan ola boshladi. 1990-yillarning boshida internet tijorat maqsadlarida foydalanishga ruxsat berilgandan so'bng kiber huquqi tez sur'attarda rivojlanib, elektron

tijorat, intellektual mulk va shaxsiy ma'lumotlarni muhofaza qilish kabi masalalar uning asosiy yo'nalishlariga aylandi.

Hozirgi kunda sun'iy intellekt, katta ma'lumotlar (Big Data), blokcheyn va Internet of Things (IoT) kabi texnologiyalar kiber huquq oldiga mutlaqo yangi muammolar va vazifalarni qo'ymoqda. Luongning qiyosiy tadqiqotida ko'rsatilganidek, zamonaviy kiber huquq nafaqat texnik muammolarni, balki jinoyatlar tasnifi va protsessual tartibga oid asosiy masalalarni ham o'z ichiga oladi[10]. Kiber huquq sohasining kelib chiqishiga quyidagi omillar sabab bo'lib xizmat qilgan:

- Virtual huquqiy munosabatlar kelib chiqishi;
- Axborot va kommunikatsiya texnologiyalarining jadal rivojlanishi;
- Axborot xavfsizligini ta'minlash zarurati;
- Raqamli iqtisodiyotga bo'gan ehtiyojning kuchayishi;
- Internetda intellektual mulk huquqini muhofaza qilish muammosi.

Kiberjinoyat — kompyuter va tarmoqlardan birgalikda foydalanish orqali sodir etiladigan jinoyat turi bo'lib, kompyuter jinoyat paytida maqsadga yo'naltirilgan qurol vazifasini bajaradi. Kiberjinoyatlar kimgadir xavfsizligi, shaxsiy daxlsizligi va moliyaviy barqarorligiga zarar yetkazish maqsadida amalga oshirilishi mumkin. Mashhur amerikalik investor Uorren Baffet kiberjinoyatni "insoniyatning birinchi raqamli muammosi" deb ta'rif bergan va "insoniyat uchun real xavf tug'diradi", deb qo'shimcha qilgan. Kanadalik huquqshunos va maslahatchi Jon Bandler o'zining keng e'tiborga sazovor bo'gan ilmiy tadqiqotida har bir tashkilot va jismoniy shaxs uchun dolzarb bo'gan uchta asosiy kiber jinoyat tahdidini alohida ajratib ko'rsetgan[11]:

– Ma'lumotlarning buzilishi (Data Breach);
– To'lov talab qiluvchi zararli dasturlar (Ransomware);
– Elektron pochtaga asoslangan pul o'tkazmalari firibgarliklari (Business Email Compromise — BEC).

McAfee homiyligida 2014-yilda chop etilgan hisobotga ko'ra, kiberjinoyatlar jahon iqtisodiyotiga yiliga 445 milliard dollar zarar yetkazgan[12]. Cybersecurity Ventures tahminlariga ko'ra, ushbu zarar 2021-yilga kelib 6 trillion dollarga, 2025-yilga borib esa 10,5 trillion dollarga yetishi kutilgan edi — va bu tahminlar amalda tasdiqlandi. Zararli dastur (Malware) hujumlari 2016-yildan 2021-yilgacha 71 foizga oshdi. 2022–2023-yillarda to'lov dasturlari (Ransomware) hujumi qurbonlari 128,17 foizga ko'paydi. 2023-yilda katta ko'lamli ma'lumotlar buzilishining eng yirik holatlari quyidagilarni o'z ichiga oladi:

- DarkBean (Kiberxavfsizlik, Buyuk Britaniya): 3,8 milliard yozuv
- Real Estate Wealth Network (Qurilish, AQSh): 1,5 milliard yozuv;
- Indian Council of Medical Research (Sog'liqni saqlash, Hindiston): 815 million yozuv;
- Kid Security (IT xizmatlari, Qozog'iston): 300 million yozuv;
- TwitterFab (IT xizmatlari, AQSh): 220 million yozuv.

2022-yil mart oyida 3 581 nafar katta yoshli amerikalik o'rtasida Pew Research Center tomonidan o'tkazilgan so'rov natijalariga ko'ra, amerikaliklar o'ntasidan yettitasi boshqa mamlakatlardan kiberhujumlar (71%) va internetda noto'g'ri ma'lumotlarning tarqalishini (70%) mamlakat oldidagi asosiy tahdid sifatida baholagan. Buyuk Britaniya hukumatining so'nggi hisobotiga ko'ra, 2023–2024-yillarda mamlakat korxonalari taxminan 7,78 million kiberjinoyat hodisasiga duch kelgan, bu esa kuniga o'rtacha 21 315 ta kiberhujumga to'g'ri keladi. 2023-yil sentabrda n yil davomida Angliya va Uelsdagi politsiyaga kompyuterdan noto'g'ri foydalanish bo'yicha taxminan 898 000 ta xabar berilgan — bu 2022-yildagiga nisbatan 30 foizga ko'p[13]. So'ngi uch yil davomida Oksford universiteti tomonidan

o'tkazilgan tadqiqotlar asosida Dunyo Kiberjinoyatlar Indeksi (World Cybercrime Index, WCI) tuzildi. Unda 92 nafar xalqaro ekspertning baholashlari umumlashtirildi. Natijalar shuni ko'rsatadiki, birinchi o'rinni Rossiya Federatsiyasi (58,39 ball) egallagan; undan keyin Ukraina (36,44 ball), Xitoy (27,86 ball), AQSh (25,01 ball) va Nigeriya (21,28 ball) joylashgan[14]. Global kiberjinoyatlar o'chog'ining o'ntaligiga Ruminiya (14,83), Shimoliy Koreya (10,61), Britaniya (9,01) va Braziliya (8,93) ham kiradi.

Xalqaro hamjamiyat kiberjinoyatlarga qarshi kurashishda bir qator muhim huquqiy hujjatlarni qabul qildi. Ushbu hujjatlar turli yondashuvlarni aks ettiradi: ba'zilarini faqat mintaqaviy, boshqalarini esa global xarakter kasb etadi. Toshkent davlat yuridik universitetida o'tkazilgan ilmiy tadqiqotlar bu sohadagi huquqiy tartibga solish masalalarini maxsus muhokama qilishga imkon bergan[15].

Budapesht konvensiyasi 2001-yil 23-noyabrda qabul qilingan "Kiberjinoyatchilik to'g'risidagi Konvensiya" ya'ni Budapesht konvensiyasi — kiberjinoyatlarga qarshi xalqaro huquqiy kurashning asosiy hujjati hisoblanadi[16]. Uning asosiy maqsadi kiberjinoyatlar bo'yicha milliy qonunchilikni uyg'unlashtirish va davlatlar o'rtasidagi hamkorlikni mustahkamlashdan iborat. 2025-yil holatiga ko'ra ushbu konvensiyani 78 ga yaqin davlat ratifikatsiya qilgan, jumladan Argentina, Avstraliya, Isroil, Yaponiya, AQSh va 50 dan ortiq boshqa davlatlar.

Konvensiyaning 23-moddasida xalqaro hamkorlik tartibi belgilab qo'yilgan, unga ko'ra, tomonlar jinoiy ishlar bo'yicha tergov yoki ish yuritish, shuningdek elektron shaklda jinoiy dalillarni yig'ish uchun bir-biri bilan maksimal darajada hamkorlik qilishlari shart. Konvensiyaning 37-moddasida esa yangi davlatlarning hujjatga qo'lilish tartibi belgilangan: Yevropa Kengashi Vazirlar Qo'lmitasi barcha ahdlashuvchi tomonlarning bir ovozdan roziligi bilan yangi davlatni taklif qilishi mumkin. Konvensiya tomonlari kompyuter tizimlarining maxfiyligi, yaxlitligi va mavjudligini ta'minlash, axborot sohasidagi jinoyatlarni aniqlash, tergov qilish hamda xalqaro hamkorlikni mustahkamlash majburiyatlarini o'z zimmalariga olgan.

Shuni ta'kidlash zarurki, O'zbekiston Respublikasi va Rossiya Federatsiyasi ushbu konvensiyani hali ratifikatsiya qilmagan. Konvensiyaga qarshi bo'lganlarning asosiy e'tirozi davlat suverenitetining buzilishiga taalluqlidir. Konvensiya doirasida ba'zi harakatlar ushbu harakatlar amalga oshiriladigan davlat hududidagi tomonni oldindan ogohlantirilmasdan va uning roziligisiz bajarilishi mumkin deb belgilangan. Budapesht konvensiyasining asosiy maqsadlari:

- Kiberjinoyatlar bo'yicha yagona xalqaro huquqiy baza yaratish;
- Milliy qonunchilikni xalqaro standartlar bilan uyg'unlashtirish;
- Davlatlar o'rtasida samarali hamkorlikni yo'lga qo'yish;
- Raqamli muhitda xavfsizlik va ishonchni mustahkamlash.

Palermo konvensiyasi BMTning 2000-yilda qabul qilingan "Transmilliy tashkil etilgan jinoyatchilikka qarshi konvensiyasi" kiberjinoyatlar sohasiga to'g'ridan-to'g'ri bag'ishlanmagan bo'lib, u yanada keng — uyushgan jinoyatchilik — kontekstida xalqaro hamkorlikni tartibga solidi[17]. Biroq uyushgan kiberjinoyatchilik guruhlari faoliyati, kiberterorizm va kiberfiribgarlikning keng ko'lamli turlari aynan ushbu konvensiya mexanizmlari orqali ham tartibga solinishi mumkin. Konvensiyani bugungi kunda 189 ta davlat ratifikatsiya qilgan, bu esa uni amalda universallik darajasiga yetkazadi.

BMT ning kiberjinoyatlar konvensiyasi loyihasi 2019-yildan boshlab BMT doirasida kiberjinoyatlarga qarshi yagona universal konvensiya ishlab chiqish bo'yicha maxsus jarayon boshlandi. UNODC tadqiqotida ta'kidlanganidek, yagona universal hujjatning yo'qligi xalqaro

hamkorlikdagi asosiy muammo bo'lib, yangi BMT konvensiyasining muvaffaqiyati barcha davlatlarning siyosiy ishtiroki va darajasiga bog'liq. Hozirgi kunda ushbu hujjat loyihasi muzokaralar bosqichida bo'lib, uning kuchga kirishi xalqaro kiber huquq sohasida fundamental o'zgarishlarga olib kelishi kutilmoqda. Ushbu yangi hujjat qabul qilingandan keyin O'zbekiston ham uni ratifikatsiya qilib qonunchiligiga implementatsiya qilish imkoniyatiga ega bo'ladi.

O'zbekiston Respublikasi kiberjinoyatlarga qarshi milliy qonunchilikni shakillantirish jarayonida muhim qadamlar qo'ymagan deb bo'lmaydi. Jinoyat kodeksining XXI bobi to'g'ridan-to'g'ri axborot texnologiyalari sohasidagi jinoyat normalarini o'z ichiga oladi. Jumladan, ushbu bobda quyidagilar uchun jinoiy javobgarlik belgilangan:

- Axborotlashtirish qoidalarini buzish (278^1-modda);
- Kompyuter axborotidan ruxsatsiz foydalanish;
- Ruxsatsiz kirish uchun maxsus vositalarni tayyorlash, o'tkazish va tarqatish;
- Kompyuter axborotini o'rinsiz modifikatsiyalashtirish;
- Kompyuter sabotaji;
- Zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish.

Biroq tahlil shuni ko'rsatadiki, mavjud sanksiyalar kiberjinoyatlarning haqiqiy ijtimoiy xavfliligiga mutanosib kelmaydi. Masalan, Jinoyat kodeksining 278^1-modda bo'yicha "axborotlashtirish qoidalarini buzish" uchun belgilangan jazo bazaviy hisoblash miqdorining ellik baravarigacha jarima yoki 1 yilgacha axloq tuzatish ishlaridan iborat. Holbuki xalqaro amaliyotda bunday jinoyatlar uchun ancha og'irroq sanksiyalar ko'zda tutiladi. UNODCning keng qamrovli tadqiqotida ta'kidlanganidek, Budapesht konvensiyasiga a'zo bo'lmagan davlatlarda jinoyatlar tasnifi ham, sanksiyalar darajasi ham xalqaro taqqosiy huquq normalariga to'liq muvofiq kelmaydi. O'zbekistonlik olim Atkhamjonov ham shu muammoni alohida qayd etib, milliy qonunchilik islohotlari xalqaro standartlarga to'liq erishishni endigina boshlayotganini ta'kidlaydi.

Bundan tashqari, O'zbekiston "Elektron hukumat to'g'risida"gi Qonun va bir qator prezident qarorlarini ham qabul qilgan. So'ngi yillarda O'zbekistonda kiberxavfsizlik sohasidagi me'moriy infratuzilma ham shakillandi hamda Axborot xavfsizligi markazi va tegishli idoralarning funksiyalari kengaytirildi. Biroq milliy qonunchilikni xalqaro konvensiyalar bilan uyg'unlashtirish jarayoni hali yakunlanmagan. Ilmiy izlanishni olib brogan olimlar bu masalada O'zbekiston uchun eng muhim qadam sifatida xalqaro standartlarga muvofiq islohotlarni tezlashtirish, jumladan Budapesht konvensiyasiga qo'bshilish jarayonini boshlashni tavsiya qiladi.

Xalqaro konvensiyalarning milliy qonunchilikka implementatsiyasi nafaqat rasmiy ratifikatsiya qilishni, balki uning mohiyatini ham ichki huquq tizimiga singdirish jarayonini o'z ichiga oladi. Bu jarayon ko'plab davlatlar uchun jiddiy muammolarni tug'diradi. Budapest konvensiyasi bilan qiyosiy tahlilida ko'rsatilganidek, konvensiyaning muvaffaqiyatli implementatsiyasi uchun davlat faqat normalarni rasmiy qonunga kiritishi yetarli emas, u bir vaqtning o'zida tergov salohiyatini, huquqiy amaliyotni va xalqaro hamkorlik mexanizmlarini ham mustahkamlashi shart. ham kiberjinoyat qonunchiligiga oid qiyosiy tadqiqotida huquqiy tizim va institutsional salohiyat o'rtasidagi muvofiqlik implementatsiyaning asosiy sharti ekanligini alohida ko'rsatib bergan [3].

O'zbekiston amaliyotida esa my.sud.uz portali orqali tahlil qilingan sud qarorlar shuni ko'rsatadiki, kiberjinoyatlar sohasidagi ko'pchilik ishlar, ayniqsa transchegaraviy xarakter kasb etganlari sud muhlatlari uzayib, isbotlash jarayonida jiddiy muammolarga duch kelinmoqda. Raqamli dalillarni to'plash va ularni sud tartibida ko'rib chiqish metodologiyasi

hali etarlicha ishlab chiqilmagan. Atkhamjonov O'zbekiston amaliyotini tahlil qilib, raqamli dalillar bilan ishlash va kiberforenzika bo'yicha maxsus protsessual me'yorlar hamda tergov organlarining salohiyatini oshirish zarurligini alohida ta'kidlagan[6].

Yuqoridagi tahlillardan ko'rinib turibdiki, kiberjinoyatlarning global va transchegaraviy tabiati ularni faqat milliy darajada tartibga solishni amalda imkonsiz qiladi. Xalqaro hamkorlik, xususan xalqaro konvensiyalar va ikki tomonlama shartnomalar mexanizmi orqali muqarrar bo'lib qolmoqda. Biroq mavjud xalqaro hujjatlar ham bir qator kamchiliklardan xoli emas. Bert-Jaap Koops bu masalada "xalqaro kiberjinoyat huquqining parchalaganlik holati global tahdidlarga munosib javob berishni tizimli ravishda to'smoqda" deb asoslangan xulosa chiqaradi[18].

Birinchi muammo sifatida universal qamrovning yoqligini ko'rsatish mumkin. Budapesht konvensiyasi Rossiya, Xitoy va boshqa bir qator yirik davlatlarni o'z ichiga olmaydi. Bu esa amalda eng ko'p kiberjinoyatlar kelib chiqadigan hududlarda xalqaro hamkorlikning samarali amalga oshirilishini to'sib qo'ymoqda. WCI ma'lumotlariga ko'ra, birinchi o'rinlarni egallagan Rossiya va Xitoy hozircha Budapesht konvensiyasiga a'zo emas[19]. Ikkinchi muammo — texnologiyaning huquqdan tez rivojlanishi. Sun'iy intellekt yordamida amalga oshiriladigan hujumlar, deepfake texnologiyasi, neyron tarmoqlarga asoslangan firibgarliklar bularning barchasi amaldagi konvensiyalarda ko'zda tutilmagan holatlarga taalluqli. Bandler kiberjinoyatlarga oid huquqiy tartibga solish texnologik rivojlanish sur'atiga to'qnasha olmasligini, bu esa tashkilotlar va jismoniy shaxslarni yangi tahdidlar oldida zaif qoldirishini alohida ta'kidlagan. Uchinchi muammo — VPN va Darknet masalasi. Hozirda ko'pchilik kiberjinoyatlar VPN va Tor kabi vositalar orqali sodir etilmoqda. Rossiya, Xitoy, Eron, Turkmaniston kabi bir qator davlatlar VPN dan foydalanishni qisman yoki to'liq bloklagan. Biroq bu yondashuv ham eng samarali yechim bo'lmasligi mumkin. Chunki tajribali kiberjinoyatchilar blokirovkani chetlab o'tish yo'llarini topadi, oddiy fuqarolar esa o'zlarining qonuniy raqamli huquqlaridan mahrum bo'ladi.

XULOSA

Kiberjinoyatchilik XXI asrning eng jiddiy global tahdidlaridan biriga aylangan bo'lib, uni faqat milliy qonunchilik doirasida bartaraf etish iloji yo'q. Xalqaro konvensiyalar, xususan Budapesht konvensiyasi xalqaro hamkorlikning muhim huquqiy asosini tashkil qilsada, ularning universal qamrovi hali to'liq ta'minlanmagan. O'zbekiston milliy qonunchiligi esa xalqaro standartlarga muvofiqlashtirish nuqtai nazaridan bir qator tizimli islohotlarni talab qilmoqda.

Ushbu tadqiqot natijalari asosida bir nechta o'zaro bog'liq takliflar ilgari suriladi. Birinchi navbatda, O'zbekiston hukumati Budapesht konvensiyasini ratifikatsiya qilish imkoniyatini jiddiy ko'rib chiqishi zarur, chunki xalqaro hamkorlikdan keladigan foydalar, masalan, operativ ma'lumot almashinuv, qo'shma tergov va ekstraditsiya mexanizmlari mumkin bo'gan suveren cheklovlardan sezilarli darajada ustun turadi. Shu bilan birga amaldagi Jinoyat kodeksidagi, xususan 278^1-modda bo'yicha belgilangan, sanksiyalar kiberjinoyatlarning haqiqiy ijtimoiy xavfliligiga mutanosib kelmaydi va ularni kuchaytirish zarur islohotlardan biri hisoblanadi. BMT yoki Interpol esa barcha a'zo davlatlarning bunday guruhlari uchun yagona malaka oshirish dasturini muvofiqlashtirishi maqsadga muvofiqdir. Raqamli tahdidlarni erta aniqlash va oldini olish uchun milliy kiberxavfsizlik tizimiga sun'iy intellektga asoslangan monitoring va tahlil vositalarini joriy etish ham dolzarb vazifalardan bo'lib, bu borada o'z ishlab chiqish bilan bir qatorda xalqaro tajribalardan foydalanish ko'zda tutilishi kerak. VPN masalasida esa yagona "taqiqlash" yondashuvi yetarli emas: qonuniy maqsadlarda VPN dan foydalanishga aniq tartib joriy etilishi, biroq Darknet va noqonuniy maqsadlarda foydalanish uchun munosib jinoiy sanksiyalar belgilanishi, shuningdek foydalanuvchi

ma'lumotlarini uchinchi tomonlarga sotuvchi VPN xizmatlari uchun javobgarlik ham qonunchilikda to'liq o'z aksini topishi zarur. Nihoyat, kiberjinoyatlarning aksariyati foydalanuvchilarning e'tiborsizdagi harakatlari natijasida yuz berishi sababli, milliy miqyosda aholining raqamli savodxonligi va huquqiy madaniyatini oshirish bo'yicha tizimli dastur amalga oshirilishi hamda ta'lim tizimining barcha bosqichlarida — maktabdan oliy ta'limgacha kiberxavfsizlik va kiber huquq asoslarini o'rgatish majburiy komponentga aylantirilishi kerak. Ushbu takliflar birgalikda amalga oshirilganida O'zbekiston raqamli xavfsizlik sohasida sezilarli yutuqlarga erisha oladi va xalqaro hamkorlik tizimida to'laqonli ishtirokchi bo'lishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. International Telecommunication Union. (2024). Global internet usage statistics 2024. ITU Publications.
2. World Economic Forum. (2020). The global risks report 2020 (15th ed.). World Economic Forum.
3. Clough, J. (2015). Principles of cybercrime (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139540803
4. Koops, B.-J., & Brenner, S. W. (Eds.). (2006). Cybercrime and jurisdiction: A global survey. T.M.C. Asser Press.
5. UNODC. (2013). Comprehensive study on cybercrime (Draft, February 2013). United Nations Office on Drugs and Crime. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
6. Atkhamjonov, A. (2025). Legal and institutional foundations for combating cybercrime in the context of New Uzbekistan. American Journal of Education and Learning, 3(5), 433–441. https://advancedscienti.com/index.php/AJEL/article/view/1951
7. OSCE. (2025, November 13). Central Asian countries strengthen regional co-operation on electronic evidence. https://www.osce.org/secretariat/60115
8. Shakurov, R. R., & Vohidov, M. M. (2022). Kiber huquq — huquq sohasi sifatida: risola. O'zbekiston Respublikasi Adliya vazirligi qoshidagi Yuristlar malakasini oshirish markazi.
9. Clough, J. (2015). Principles of cybercrime (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139540803
10. Luong, H. T. (2019). Cybercrime in legislative perspectives: A comparative analysis between the Budapest Convention and Vietnam regulations. International Journal of Advanced Research in Computer Science, 10(3), 1–12. https://doi.org/10.26483/ijarcs.v10i3.6414
11. Bandler, J. (2021). Cybercrime investigations: A comprehensive resource for everyone. CRC Press. https://johnbandler.com/cyberlawbook/
12. McAfee. (2014). Net losses: Estimating the global cost of cybercrime. Intel Security.
13. Pew Research Center. (2022, June 6). Americans see different global threats facing the country now than in March 2020. https://www.pewresearch.org/short-reads/2022/06/06/americans-see-different-global-threats-facing-the-country-now-than-in-march-2020/
14. Office for National Statistics. (2023). Crime in England and Wales: Year ending September 2023. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2023
15. PhoenixPublication. (2023). Kiberjinoyatchilik sohasidagi jinoyatlar uchun javobgarlikni takomillashtirish. https://phoenixpublication.net/index.php/TANQ/article/view/1556/1316

16. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). https://rm.coe.int/1680081561
17. United Nations. (2000). Convention against transnational organized crime (Palermo Convention) (UN Doc. A/RES/55/25). https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html
18. Brenner & Koops (2004/2007) — "Approaches to Cybercrime Jurisdiction", *Journal of High Technology Law*, Vol. 4