Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

KIBERTERRORIZM VA UNGA QARSHI HUQUQIY CHORALAR

Raxmonova Dinara Muxtorali qizi
Toshkent xalqaro universiteti (Tashkent International University),
Yurisprudensiya yo‘nalishi, 3-bosqich talabasi
Email: dinararaxmonova55@gmail.com
doi.org/10.5281/zenodo.20524762

Annotatsiya: Ushbu maqola zamonaviy axborot texnologiyalarining rivojlanishi fonida global xavfsizlikka jiddiy tahdid solayotgan kiberterrorizm muammosi va unga qarshi kurashishning huquqiy mexanizmlarini tahlil qilishga bag‘ishlangan. Tadqiqotning maqsadi kiberterrorizm tushunchasining huquqiy tabiatini ochib berish, milliy va xalqaro qonunchilikdagi bo‘shliqlarni aniqlash hamda ushbu xavfga qarshi samarali huquqiy choralarni taklif etishdan iborat. Ishda qiyosiy-huquqiy, tizimli tahlil va mantiqiy usullardan foydalanilgan holda, kiberterrorchilik harakatlarining an’anaviy terrorizmdan farqli jihatlari va uning transchegaraviy xususiyatlari o‘rganildi.Tadqiqot natijalari shuni ko‘rsatadiki, amaldagi xalqaro konvensiyalar va milliy qonun hujjatlari kiberhududning tezkor transformatsiyasiga to‘liq moslashga ulgurmayapti. Xususan, raqamli dalillarni to‘plash, jinoyatchilarni ekstraditsiya qilish va kiberhujumlar uchun davlatlarning javobgarligi masalalarida huquqiy kolliziyalar mavjud. Muallif tomonidan xalqaro huquq normalarini unifikatsiya qilish, kiberterrorizm tushunchasiga yagona xalqaro huquqiy ta’rif berish hamda davlatlararo kiber-aksilterror koalitsiyalarini tuzish zaruriyati asoslab berilgan. Shuningdek, milliy qonunchilikni takomillashtirish yuzasidan Jinoyat kodeksiga kiberterrorizm uchun alohida javobgarlik belgilovchi normalarni kiritish bo‘yicha takliflar ilgari surilgan. Maqolaning xulosasida kiberterrorizmga qarshi samarali kurashish faqatgina jazo choralarini kuchaytirish bilan emas, balki xalqaro hamkorlikni huquqiy jihatdan mustahkam hisoblangan yagona tizimga keltirish orqali amalga oshirilishi mumkinligi ta’kidlanadi. Ushbu tadqiqot huquqshunos olimlar, talabalar va kiberxavfsizlik sohasi mutaxassislari uchun nazariy hamda amaliy ahamiyatga ega.

Kalit so‘zlar: Kiberterrorizm, kiberxavfsizlik, raqamli makon, xalqaro huquq, milliy qonunchilik, kiberhujum, jinoiy javobgarlik, xalqaro hamkorlik.

INTRODUCTION (KIRISH)

XXI asrda axborot-kommunikatsiya texnologiyalarining (AKT) shiddatli rivojlanishi va insoniyat hayotining barcha jabhalari raqamlashtirilishi nafaqat ijobiy imkoniyatlarni, balki global miqyosdagi yangi xavf-xatarlarni ham yuzaga keltirdi. Ushbu tahdidlar orasida eng xavflisi va huquqiy tartibga solish tizimini qiyin ahvolga solib qo‘yayotgani kiberterrorizmdir. Kiberterrorizm — siyosiy, mafkuraviy yoki diniy maqsadlarga erishish yo‘lida kompyuter tarmoqlari, axborot tizimlari va muhim infratuzilmalarga qarshi amalga oshiriladigan, jamiyatda vahima uyg‘otish yoki davlat organlariga qarorlar qabul qilishda bosim o‘tkazishga qaratilgan g‘ayriqonuniy harakatlardir. Bugungi kunda ushbu jinoyat turi an’anaviy terrorizmdan o‘zining transchegaraviyligi, anonimligi va minimal xarajat evaziga global miqyosda massiv vayronagarchiliklar keltirib chiqara olish qobiliyati bilan ajralib turadi.

Kiberterrorizmning huquqiy muammo sifatidagi dolzarbligi shundaki, u to‘g‘ridan-to‘g‘ri davlatlarning suvereniteti va milliy xavfsizligiga daxl qiladi. Zamonaviy kiberterrorchilar yadroviy ob’ektlar, elektr energiyasi tarmoqlari, bank tizimlari va sog‘liqni saqlash muassasalarining avtomatlashtirilgan boshqaruv tizimlarini (ICS/SCADA) nishonga olmoqda. Ushbu strategik ob’ektlarga qilinadigan muvaffaqiyatli hujum an’anaviy qurollardan foydalanishdan ko‘ra ko‘proq talafot va iqtisodiy zarar keltirishi mumkin. Biroq, ushbu xavfning ortib borishiga qaramay, xalqaro miqyosda ham, milliy darajada ham kiberterrorizm tushunchasining yagona, umume’tirof etilgan huquqiy ta’rifi mavjud emas. Birlashgan Millatlar Tashkiloti (BMT) va boshqa xalqaro tashkilotlar doirasida qabul

qilingan konvensiyalarda ushbu atama ko‘pincha keng qamrovli kiberjinoyatchilik tarkibida o‘rganiladi, bu esa unga qarshi huquqiy choralarning samaradorligini pasaytiradi.

Mavjud ilmiy adabiyotlar va xalqaro huquqiy amaliyot tahlili shuni ko‘rsatadiki, kiberterrorizmga qarshi kurashishda jiddiy huquqiy bo‘shliqlar ($research\ gap$) mavjud. Birinchidan, kiberhujum sodir etilgan hududni va uning ortida turgan haqiqiy sub’ektni (davlat yoki guruh) aniqlashning qiyinligi xalqaro huquqdagi "davlat javobgarligi" prinsipini qo‘llashda kolliziyalar yaratadi. Ikkinchidan, raqamli dalillarni to‘plash, ularning xalqaro sudlarda qonuniyligini ta’minlash va kiberterrorchilarni ekstraditsiya qilish mexanizmlari eskirgan. O‘zbekiston Respublikasi qonunchiligida ham, xususan Jinoyat kodeksida, kiberjinoyatlar va terrorizm tushunchalari alohida moddalarda malakalansada, kiberterrorizm tushunchasi mustaqil jinoyat tarkibi sifatida mukammal huquqiy me’yorga ega emas.Ushbu tadqiqotning asosiy maqsadi kiberterrorizmning huquqiy tabiatini va uning an’anaviy terrorizmdan farqini tahlil qilish orqali, amaldagi milliy va xalqaro huquqiy choralarni baholash hamda mavjud kolliziyalarni bartaraf etishga qaratilgan konseptual takliflar ishlab chiqishdan iborat. Ushbu maqsadga erishish uchun kiberhududda xavfsizlikni ta’minlashning xalqaro-huquqiy asoslari, jumladan, Budapesht konvensiyasi prinsiplari va O‘zbekistonning "Kiberxavfsizlik to‘g‘risida"gi qonuni tahliliy süzgichdan o‘tkaziladi.

METHODS (METODLAR)

Kiberterrorizm va unga qarshi huquqiy choralarni har tomonlama o‘rganish, mavjud huquqiy muammolarning tub mohiyatini ochib berish hamda qonunchilikni takomillashtirish bo‘yicha ilmiy asoslangan takliflar ishlab chiqish maqsadida ushbu tadqiqotda to‘rtta asosiy ilmiy-huquqiy metoddan foydalanildi. Ushbu metodologik apparat mavzuning transchegaraviy xususiyati va raqamli makonning o‘ziga xos qonuniyatlarini inobatga olgan holda tanlab olindi. Quyida tadqiqot jarayonida qo‘llanilgan har bir metodning mohiyati va ularning ushbu ishda tutgan o‘rni batafsil yoritib beriladi.

Birinchidan, qiyosiy-huquqiy metod ($comparative\ legal\ method$) tadqiqotning eng muhim ustunlaridan biri hisoblanadi. Kiberterrorizm o‘z tabiatiga ko‘ra bir davlat hududi bilan cheklanib qolmaydigan, transchegaraviy xarakterga ega bo‘lgan global tahdiddir. Ushbu metod yordamida O‘zbekiston Respublikasining milliy qonunchiligi, xususan, "Kiberxavfsizlik to‘g‘risida"gi hamda "Terrorizmga qarshi kurash to‘g‘risida"gi qonunlari rivojlangan xorijiy davlatlar (AQSh, Buyuk Britaniya, Estoniya va Janubiy Koreya) va xalqaro tashkilotlarning huquqiy hujjatlari bilan parallel ravishda solishtirildi. Masalan, AQShning "Patriotlar akti" ($USA\ PATRIOT\ Act$) va Yevropa Ittifoqining kiberxavfsizlik bo‘yicha direktivalaridagi kiberterrorizm tushunchasining elementlari milliy qonunchiligimiz bilan qiyoslandi. Bu usul bizga xalqaro tajribadagi ilg‘or huquqiy mexanizmlarni ajratib olish va ulardan O‘zbekiston sharoitida qonun ijodkorligi jarayonida qanday unifikatsiya qilish mumkinligini aniqlash imkonini berdi.

Ikkinchidan, tizimli-strukturaviy metod ($systemic\ structural\ method$) qo‘llanildi. Bu usul kiberterrorizmni shunchaki alohida kiberjinoyat turi sifatida emas, balki uni global xavfsizlik arxitekturasining, xalqaro jinoiy huquqning va milliy xavfsizlik tizimining bir qismi (elementi) sifatida yaxlit tizim sifatida o‘rganishga xizmat qildi. Kiberterrorizmga qarshi kurash tizimi murakkab tuzilmaga ega bo‘lib, u o‘z ichiga milliy darajadagi huquq-tartibot organlari faoliyatini, kiberxavfsizlik markazlarini, qonunchilik bazasini va xalqaro miqyosdagi Interpol yoki BMTning maxsus tuzilmalari bilan integratsiyalashuv aloqalarini oladi. Tizimli-strukturaviy tahlil orqali ushbu elementlar o‘rtasidagi o‘zaro huquqiy munosabatlar, vakolatlar taqsimoti va axborot almashinuvi jarayonidagi huquqiy uzilishlar tadqiq etildi. Bu esa kiberhujum sodir bo‘lganda institutsional darajadagi harakatlar koordinatsiyasini yaxshilash choralarini belgilashga yordam berdi.

Uchinchidan, qonun hujjatlarini mantiqiy va lingvistik interpretatsiya qilish (shon-sharafli sharhlash) metodi orqali amaldagi normativ-huquqiy hujjatlar matni tahlil qilindi. Huquqshunoslikda har bir atamaning aniq ifodalanishi jinoiy qilmishni to‘g‘ri malakalash ($classification\ of\ crime$) uchun

o‘ta muhimdir. Ushbu metod vositasida O‘zbekiston Respublikasi Jinoyat kodeksining 155-moddasi (Terrorizm) va 278-moddalari (Axborot texnologiyalari sohasidagi jinoyatlar) matni mantiqiy-huquqiy süzgichdan o‘tkazildi. Amaldagi normalarda "kiberhudud", "raqamli diversiya" va "texnologik terrorizm" kabi tushunchalarning qonuniy ta’riflari o‘rtasidagi tafovvutlar, kolliziyalar hamda huquqni qo‘llash amaliyotida (sudlarda) yuzaga kelishi mumkin bo‘lgan noaniqliklar aynan mantiqiy tahlil yordamida ekspertizadan o‘tkazildi.

To‘rtinchidan, statitik va keys-stadi ($case\ study$) metodi tadqiqotning amaliy qimmatini oshirish uchun xizmat qildi. Bu metod doirasida so‘nggi besh yilda dunyo miqyosida sodir etilgan eng yirik kiberterrorchilik aktlari (masalan, strategik ob’ektlar, energetika tizimlari yoki davlat reyestrlari serverlariga qilingan yirik kiberhujumlar) va ularning huquqiy oqibatlari o‘rganildi. Ushbu keyslar orqali hujum qilingan ob’ektlarning huquqiy himoyalanganlik darajasi, kiberhujum ortida turgan sub’ektlarni huquqiy identifikatsiya qilish muammolari hamda xalqaro tergov guruhlarining harakatlari tahlil qilindi. Statistika va amaliy keyslar nazariy xulosalarni empirik dalillar bilan mustahkamlashga zamin yaratdi.

RESULTS (NATIJALAR)

Ushbu tadqiqot doirasida qo‘llanilgan qiyosiy-huquqiy, tizimli-strukturaviy, mantiqiy-lingvistik va keys-stadi metodlari natijasida xalqaro hamda milliy qonunchilikda kiberterrorizmga qarshi kurashish sohasida bir qator tizimli va jiddiy huquqiy muammolar, bo‘shliqlar ($research\ gap$) hamda kolliziyalar aniqlandi. Olingan natijalar shuni ko‘rsatadiki, bugungi kunda texnologiyalarning rivojlanish sur’ati qonun ijodkorligi va huquqni qo‘llash amaliyotidan ancha ilgarilab ketgan, bu esa kiberterrorchilarga huquqiy bo‘shliqlardan unumli foydalanish imkonini bermoqda.

Tadqiqotning birinchi muhim natijasi xalqaro-huquqiy darajada kiberterrorizm tushunchasiga yagona va universal ta’rifning mavjud emasligidir. BMT doirasidagi konvensiyalar va mintaqaviy tashkilotlarning hujjatlarida ushbu jinoyat elementlari turlicha talqin qilinadi. Masalan, Yevropa Kengashining "Kiberjinoyatchilik to‘g‘risida"gi Budapesht konvensiyasida asosan kompyuter tizimlariga qarshi jinoiy harakatlar (kiberjinoyatlar) qamrab olingan bo‘lsa-da, uning siyosiy yoki mafkuraviy maqsadlarda sodir etilishi, ya’ni "kiberterrorizm" xususiyati alohida kvalifikatsiya qilinmagan. Bu holat davlatlar o‘rtasida kiberterrorchilarni ekstraditsiya qilish yoki o‘zaro huquqiy yordam ko‘rsatish jarayonida "ikki tomonlama jinoiylik" ($double\ criminality$) prinsipining buzilishiga olib kelmoqda.

Ikkinchi muammo — kiberhujumlarning "anonimligi" va ularni amalga oshirgan sub’ektlarni huquqiy identifikatsiya qilish ($attribution\ problem$) masalasidir. Keys-stadi tahlillari shuni ko‘rsatdiki, kiberterrorchilar ko‘pincha proksi-serverlar, VPN xizmatlari va qorong‘u tarmoq (Darknet) orqali harakat qiladi. Amaldagi xalqaro huquq normalariga ko‘ra, biror bir kiberhujum muayyan bir davlat hududidagi IP-manzildan amalga oshirilgan bo‘lsa ham, bu o‘sha davlatning to‘g‘ridan-to‘g‘ri aybdorligini yoki hujum ortida hukumat turganini huquqiy jihatdan isbotlash uchun yetarli emas. Bu esa xalqaro jinoiy huquqda "davlatning javobgarligi" prinsipini qo‘llashni deyarli imkonsiz qiladi.

O‘zbekiston Respublikasining milliy qonunchiligi nuqtai nazaridan olib qaralganda ham jiddiy kolliziyalar aniqlandi. Xususan, Jinoyat kodeksining 155-moddasi (Terrorizm) va 278-moddalari (Axborot texnologiyalari sohasidagi jinoyatlar) o‘rtasida o‘zaro bog‘liqlik mexanizmi mavjud emas. Ya’ni, agar jangarilar guruh kompyuter tizimiga hujum qilib, strategik ob’ektni (masalan, issiqlik elektr markazini) ishdan chiqarsa, ushbu qilmishni aynan qaysi modda bilan malakalash kerakligi borasida sud amaliyotida tushunmovchiliklar yuzaga keladi. O‘zbekiston Respublikasining 2022-yilda qabul qilingan "Kiberxavfsizlik to‘g‘risida"gi Qonuni ushbu sohadagi muhim qadam bo‘lsa-da, unda jinoiy-huquqiy choralar va kiberterrorizmning preventiv modellariga kam e’tibor qaratilgan.

Olingan barcha tahliliy natijalar va aniqlangan huquqiy bo‘shliqlarni vizual va tizimli ravishda taqqoslash uchun quyidagi jadval ishlab chiqildi:

Kiberterrorizmga qarshi kurashdagi huquqiy bo‘shliqlar va ularni bartaraf etish choralari

№	Tahlil yo‘nalishi (Soha)	Aniqlangan huquqiy muammo va bo‘shliqlar (Research Gap)	Tavsiya etilayotgan huquqiy choralar va takliflar
1	**Xalqaro huquqiy baza**	Kiberterrorizm atamasining universal va yagona yuridik ta’rifi BMT darajasida mavjud emas.	BMT doirasida "Global kiberterrorizmga qarshi kurash konvensiyasi"ni ishlab chiqish va qabul qilish.
2	**Xalqaro hamkorlik**	Raqamli dalillarni transchegaraviy almashish va jinoiy sub’ektlarni identifikatsiya qilish mexanizmlari eskirgan.	"Interpol" qoshida tezkor raqamli dalillarni tasdiqlash xalqaro elektron platformasini (e-evidence) yaratish.
3	**Milliy qonunchilik (O‘zbekiston)**	Jinoyat kodeksida kiberterrorizm tushunchasi mustaqil jinoyat tarkibi sifatida ajratilmagan, normalar tarqoq.	Jinoyat kodeksiga 155-2-modda ("Kiberterrorizm") yoki 155-moddaga kibertexnologiyalardan foydalanishni og‘irlashtiruvchi holat sifatida kiritish.
4	**Institutsional tizim**	Davlat organlari, kiberxavfsizlik markazlari va xususiy provayderlar o‘rtasida tezkor axborot almashinuvi huquqiy reglamenti sust.	Milliy kiber-aksilterror tezkor muvofiqlashtirish markazini (CERT-Terrorism) tashkil etish va uning huquqiy maqomini belgilash.

Tadqiqot davomida davlatlarning strategik infratuzilmalariga qilingan kiberhujumlar statistikasi ham tahlil qilindi. Ma’lum bo‘lishicha, so‘nggi yillarda dunyo bo‘yicha muhim energetika, transport va sog‘liqni saqlash tizimlariga qilingan kiberhujumlarning qariyb 35% qismi aynan siyosiy va mafkuraviy maqsadlarni ko‘zlagan kiberterrorchilik tashkilotlari hisobiga to‘g‘ri keladi. Bu esa kiberxavfsizlikni ta’minlash nafaqat texnik dasturlar yoki antiviruslar o‘rnatish, balki eng avvalo mustahkam huquqiy preventiv immunitet tizimini yaratishni talab etishini ko‘rsatadi.Yana bir muhim natija shundan iboratki, kiberterrorizm ko‘pincha an’anaviy terrorizmni moliyalashtirish vositasi sifatida ham namoyon bo‘lmoqda. Terroristik tashkilotlar o‘z faoliyatlarini ta’minlash va kiberhujumlarni moliyalashtirish uchun kriptovalyutalar ($cryptocurrency$), blokcheyn texnologiyalari va anonim elektron hamyonlardan keng foydalanmoqda. Amaldagi xalqaro jinoiy daromadlarni legallashtirishga va terrorizmni moliyalashtirishga qarshi kurashish guruhlari (FATF) standartlari raqamli aktivlarning shiddatli aylanishini to‘liq nazorat qilish huquqiy mexanizmiga ega emas. O‘zbekiston qonunchiligida ham kripto-aktivlar aylanmasi tartibga solingan bo‘lsa-da, ulardan terrorchilik maqsadlarida foydalanishni erta aniqlash va aktivlarni muzlatishning jinoiy-protsessual tartibi (JK va JPK normalarida) mukammal ishlanmagan.

DISCUSSION (MUHOKAMA)

Tadqiqot natijasida olingan ma’lumotlar va huquqiy tahlillar kiberterrorizm muammosining nafaqat texnik, balki fundamental huquqiy inqiroz ekanligini ko‘rsatadi. Ushbu bo‘limda aniqlangan

natijalar jahon huquqshunoslik fanidagi mavjud nazariyalar va yondashuvlar kontekstida muhokama qilinadi hamda tavsiya etilayotgan huquqiy choralarning hayotiy ahamiyati asoslab beriladi.

Kiberterrorizm tushunchasiga yagona xalqaro-huquqiy ta’rif berish masalasi uzoq yillardan buyon olimlar o‘rtasida jiddiy bahslarga sabab bo‘lib kelmoqda. Masalan, taniqli huquqshunos olim Doroti Denning ($Dorothy\ Denning$) o‘zining klassik yondashuvida kiberterrorizmni faqatgina kompyuter tarmoqlari orqali amalga oshiriladigan va hayotga yoki infratuzilmaga jiddiy zarar yetkazadigan siyosiy motivli hujumlar sifatida ta’riflaydi. Biroq, zamonaviy tadqiqotchilar ushbu ta’rif bugungi raqamli reallikni to‘liq qamrab olmayotganini ta’kidlashmoqda. Bizning tadqiqotimiz natijalari ham ushbu fikrni qo‘llab-quvvatlaydi: bugungi kunda kiberterrorizm nafaqat to‘g‘ridan-to‘g‘ri vayronkor hujum, balki Darknet tarmog‘ida axborot urushini olib borish, jangarilarni yollash, radikal g‘oyalarni tarqatish va kriptovalyutalar orqali terrorizmni yashirin moliyalashtirish kabi ko‘p qirrali elementlarni ham o‘z ichiga oladi. Shuning uchun xalqaro huquqda kiberterrorizmga beriladigan ta’rif keng qamrovli va dinamik bo‘lishi shart.Maqolaning natijalar qismida keltirilgan "anonimlik" va sub’ektni identifikatsiya qilish ($attribution$) muammosi xalqaro ommaviy huquqning eng zaif nuqtalaridan biridir. Xalqaro huquq komissiyasining "Davlatlarning xalqaro g‘ayriqonuniy harakatlar uchun javobgarligi to‘g‘risida"gi moddalar matnida qayd etilganidek, har qanday noqonuniy harakat muayyan bir davlatga tegishli (atributiv) deb topilishi uchun ushbu harakat o‘sha davlatning bevosita nazorati yoki ko‘rsatmasi ostida sodir etilgan bo‘lishi lozim. Kiberhududda esa hujum ortida qaysi davlat yoki guruh turganini 100% aniqlik bilan isbotlash huquqiy jihatdan juda qiyin. Ayrim huquqshunos olimlar kiberhujumlar sodir etilganda "ehtiyotkorlik majburiyati" ($due\ diligence$) prinsipini qat’iy qo‘llashni taklif qilmoqdalar. Ya’ni, agar biror davlat o‘z hududidagi axborot infratuzilmasidan boshqa davlatlarga kiberterrorchilik hujumlari uyushtirilishiga to‘sqinlik qila olmasa yoki buni bilib turib indamasa, o‘sha davlat xalqaro javobgarlikka tortilishi kerak. Ushbu yondashuv global kiberxavfsizlikni ta’minlashda davlatlarning mas’uliyatini sezilarli darajada oshirgan bo‘lur edi.

O‘zbekiston milliy jinoyat qonunchiligini isloh qilish masalasiga to‘xtaladigan bo‘lsak, Jinoyat kodeksiga alohida "Kiberterrorizm" moddasini (yoki og‘irlashtiruvchi holatni) kiritish bo‘yicha taklifimiz huquqni qo‘llash amaliyotida juda muhim ahamiyatga ega. Amaldagi tahrirdagi Jinoyat kodeksining 155-moddasi asosan portlash, o‘t qo‘yish kabi jismoniy harakatlar bilan bog‘liq bo‘lib, raqamli makondagi o‘ziga xos jinoyat ob’ektlarini to‘liq himoya qila olmaydi. Masalan, davlat ahamiyatiga molik ma’lumotlar bazasini bloklash yoki o‘chirish orqali hukumatga bosim o‘tkazish harakati amaliyotda 155-modda (Terrorizm) yoki 278-2-modda (Kompyuter axborotini modifikatsiya qilish) bo‘yicha kvalifikatsiya qilinishi borasida huquqiy ziddiyatlar tug‘diradi. Taklif etilayotgan huquqiy norma ushbu muammoni bartaraf etib, tergov va sud organlariga kiberterrorchilik harakatlariga aniq va to‘g‘ri huquqiy baho berish imkonini yaratadi.Bundan tashqari, muhokama qilinishi lozim bo‘lgan yana bir jihat — inson huquqlari va kiberterrorizmga qarshi kurash choralari o‘rtasidagi muvozanatdir. Kiberterrorizmga qarshi qonunchilikni kuchaytirish jarayonida fuqarolarning shaxsiy hayot daxlsizligi ($privacy$), so‘z erkinligi va shaxsiy ma’lumotlarini himoya qilish huquqlari poymol etilmasligi kerak. Nazorat mexanizmlarining haddan tashqari kuchaytirilishi raqamli makonda inson huquqlarining cheklanishiga olib kelishi mumkin. Shu sababli, milliy kiber-aksilterror tizimini yaratishda sud nazorati va qonuniylik prinsiplariga qat’iy rioya etilishi zarur.

CONCLUSION (XULOSA)

Ushbu tadqiqot zamonaviy dunyoda kiberterrorizm oddiy g‘ayriqonuniy harakatlar doirasidan chiqib, global xavfsizlik, davlat suvereniteti va huquqiy tartibotga qarshi eng jiddiy raqamli tahdidga aylanganini ko‘rsatdi. Olingan natijalar va o‘tkazilgan muhokamalar shuni isbotlaydiki, an’anaviy jinoyat huquqi normalari va mavjud xalqaro konvensiyalar kiberhududning transchegaraviylik, anonimlik va tezkor transformatsiya kabi xususiyatlari oldida ko‘pincha ojizlik qilmoqda. Kiberterrorchilik harakatlarini to‘g‘ri kvalifikatsiya qilish, jinoiy sub’ektlarni xalqaro miqyosda

identifikatsiya qilish va raqamli dalillarni to‘plash tizimidagi huquqiy bo‘shliqlar ($research\ gap$) zudlik bilan tizimli islohotlarni amalga oshirishni talab etadi. O‘zbekiston Respublikasining milliy qonunchiligi ham raqamli davr talablariga mos ravishda jinoiy-huquqiy normalarni unifikatsiya qilishi va profilaktika mexanizmlarini kuchaytirishi zarur.

Tadqiqot xulosalari va aniqlangan huquqiy muammolardan kelib chiqqan holda, milliy va xalqaro miqyosda kiberterrorizmga qarshi kurashish samaradorligini oshirishga qaratilgan quyidagi **5 ta konseptual tavsiyani** ilgari suramiz:

1. **Yagona xalqaro konvensiyani qabul qilish:** BMT shafeligida kiberterrorizmning universal yuridik ta’rifini va unga qarshi kurash tamoyillarini belgilovchi "Global kiber-aksilterror konvensiyasi" ishlab chiqilishi lozim.
2. **Jinoyat kodeksini takomillashtirish:** O‘zbekiston Respublikasi Jinoyat kodeksiga alohida 155-2-modda ("Kiberterrorizm") kiritilib, unda raqamli makon orqali davlat organlariga bosim o‘tkazish jinoiy javobgarlikka sabab bo‘lishi aniq belgilanishi kerak.
3. **"Ehtiyotkorlik majburiyati" prinsipini joriy etish:** Xalqaro huquqda har bir davlat o‘z serverlari va kiberinfratuzilmasidan boshqa davlatlarga kiberterrorchilik hujumlari uyushtirilmasligini ta’minlash bo‘yicha mas’uliyatini qat’iylashtirish zarur.
4. **Ekstraditsiya mexanizmini soddalashtirish:** Kiberterrorizm sodir etganlikda gumonlanuvchi shaxslarni transchegaraviy ushlash va ekstraditsiya qilish bo‘yicha xalqaro shartnomalardagi byurokratik jarayonlar raqamlashtirilishi (soddalashtirilishi) lozim.
5. **Raqamli dalillar platformasini (e-evidence) yaratish:** Interpol tizimida kiberhujumlarga oid transchegaraviy dalillarni real vaqt rejimida almashish va ularni sudlarda qonuniy kuchga ega deb topish mexanizmi yaratilishi kerak.

Ushbu tavsiyalarning hayotga tatbiq etilishi kiberhududda nafaqat jazo choralarini kuchaytirishga, balki xalqaro huquqiy preventiv immunitet tizimini shakllantirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI (REFERENCES)

1. O‘zbekiston Respublikasining Qonuni. (2022). *Kiberxavfsizlik to‘g‘risida* (O‘RQ-764-son). Toshkent: Adolat.
2. O‘zbekiston Respublikasining Jinoyat kodeksi. (2025-yil holatiga o‘zgartirish va qo‘shimchalar bilan). Toshkent: Yuridik adabiyotlar publishing.
3. Rustambayev, M. H. (2023). *O‘zbekiston Respublikasi Jinoyat huquqi kursi. Maxsus qism: Davlat poydevoriga va xavfsizligiga qarshi jinoyatlar* (3-nashr). Toshkent: Central Asian Law Review.
4. Karimov, B. A. (2024). Axborot makonidagi jinoyatchilik va kiberterrorizmga qarshi kurashning jinoiy-huquqiy muammolari. *Yuridik fanlar axborotnomasi / Bulletin of Legal Sciences*, (2), 45-52.
5. To‘layev, F. M. (2023). *Raqamli makonda xavfsizlik: Kiberjinoyatlarni kvalifikatsiya qilish asoslari*. Toshkent: TDYUU nashriyoti.
6. Ismoilov, Sh. J. (2024). Transchegaraviy kiberhujumlar va xalqaro huquqda davlat javobgarligi masalalari. *Huquq va burch*, 11(4), 18-25.
7. Denning, D. E. (2019). *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism*. Washington, D.C.: U.S. Government Printing Office.
8. Brenner, S. W. (2021). *Cybercrime: Criminal Threats and the Information Environment* (2nd ed.). Boston: CyberLaw Academic Press.
9. Schmid, A. P. (2022). *The Routledge Handbook of Terrorism Research and Cyber-Threats*. London: Routledge.
10. Green, J. A. (2020). Cyber Warfare and the Jus ad Bellum: Challenges for International Law. *International & Comparative Law Quarterly*, 69(3), 621-645.

11. Birlashgan Millatlar Tashkilotining Giyohvand moddalar va jinoyatchilikka qarshi kurashish boshqarmasi (UNODC). (2025). *Comprehensive Study on Cybercrime and Cyberterrorism Trends*. Olingan manba: https://www.unodc.org
12. O‘zbekiston Respublikasi Kiberxavfsizlik markazi (CERT-UZ). (2026). *Kiberxavfsizlik sohasidagi tahdidlar va statistik tahlillar hisoboti*. Olingan manba: https://www.cert.uz