2-TOM, 6-SON

KIBERTERRORIZMNING MARKAZIY OSIYO DAVLATLARI UCHUN XAVFI.

Abdusattorov Shahzod Abdumumin o'g'li

Ushbu tezisda kiberterrorizmning Markaziy Osiyo davlatlariga ta'siri va xavfi unga qarshi kurashda xalqaro va milliy qonunchilik tizimi, davlatlarning o'zaro hamkorligi haqida to'xtalib o'tiladi.

Kalit so'zlar: kiberterrorizm, terrorizm, Mustaqil davlatlar hamdo'stligi, Birlashgan Millatlar Tashkiloti.

Axborot texnologiyalari va ommaviy axborot vositalariga oid qonunchilik sohasidagi tadqiqotlarning jadal rivojlanishi transchegaraviy kiber tartibga solishdagi mumkin bo'lgan keskinliklarni tezkor va har tomonlama tekshirish zaruriyatini keltirib chiqardi. Ushbu keskinliklar amaldagi xalqaro qonunlarni amaliy bo'lmagan holga keltirishini aniqlash uchun zarur bo'lib, shu tariqa mavjud huquqiy bazalarni qayta ko'rib chiqish va qayta talqin qilishni talab qiladi. Sohadagi qiyinchilik kiberterrorizm tahdidining kuchayishiga qarshi kurashda xalqaro hamkorlik bo'yicha terrorizmga qarshi idoralar o'rtasida jinoiy faoliyat bilan bog'liq dalillarni almashishga ko'maklashish imperativ hamda radio va raqamli aloqa bilan bog'liq ayrim harakatlarni ushlashdan himoya qilish zarurati o'rtasidagi muvozanatni topishdan iborat. Monitoring yoki oshkor qilish, agar jamoat xavfsizligi bilan oqlangan aralashuvga majburiy ehtiyoj bo'lmasa. Ushbu qarama-qarshi muammolarni hal qilish o'rnatilgan huquqiy tamoyillarni qo'llab-quvvatlashga tayanadi, shu bilan birga xavfsizlik xavfini yumshatishga, fuqarolar erkinliklarini himoya qilishga va huquqni qo'llashga keraksiz cheklovlar qo'yish orqali to'sqinlik qilmaslikka harakat qiladi.

"Terrorizm" atamasi faqat xatti-harakatlar boshqaruv organiga, butun aholiga yoki jamiyatning turli sohalariga qaratilgan bo'lsa qo'llaniladi. Tadqiqot qiluvchi olimlar kiberterrorizmning ushbu spektrga qanday mos kelishini va raqamli sohadagi terrorchilik faoliyatining potentsial oqibatlarini tushunish uchun terrorizmni yanada kengroq tekshirishni taklif qilmoqdalar. Rossiya Federatsiyasi Axborot va fan vazirligi huzuridagi Terrorizm tadqiqotlari va tahliliy markazining xulosalariga ko'ra, terrorchilik tashkilotlari o'zlarining ichki tuzilishi, o'ziga xos ko'lami va noqonuniy operatsiyalar bilan shug'ullanishi bilan ajralib turadi[1]. Terroristik harakatlarni amalga oshirish qobiliyati bunday tashkilotlarni ajratib turadi. Jinoyat kodeksida belgilanganidek, bu tashkilotlar

[1] *Didenko AN. Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Review. 2020. [HTML]*

terrorchilik harakatini amalga oshirish maqsadida belgilangan tartibda harakat qilayotgan shaxslar yoki jamoalarni qamrab oladi. Jinoyatchilar ixtisoslashtirilgan lagerlarda o‘qitiladigan qurollar, portlovchi qurilmalar va jismoniy shaxslarga zarar yetkazishning boshqa usullaridan foydalanish bo‘yicha ko‘rsatmalar oladilar. Markaziy Osiyoning har bir davlatida internetdan foydalanish monitoringi, veb-saytlarni tsenzura qilish, internet-kafelar faoliyatini nazorat qilish, ekstremistik yoki pornografik kontentni tarqatish bilan bog‘liq ishlarni ko‘rib chiqishga katta qiziqish mavjud. Kibermakon sohasida shaxslar uchun zarar yetkazish, jinoiy faoliyat bilan shug‘ullanish, ma’lumotlarni manipulyatsiya qilish va hatto davlatning jismoniy infratuzilmasiga murakkab hujumlar uyushtirish uchun keng imkoniyatlar mavjud. Kiberterrorizmning dastlabki tarkibiy qismlarini, jinoyat sodir etish va terrorizm bilan yaqqol aloqadorlik sifatida aniqlash mumkin, bu esa pirovardida jinoiy harakatning motiviga asoslanadi. Terrorizmning turli shakllari, asosan, jinoiy harakatlar ekanligini hisobga olsak, vaziyat yanada oydinlashadi. Keling, vaziyatni chuqurroq tahlil qilaylik. G‘arb olimlari terrorchilar zamonaviy texnologiyalardan foydalanishga, shuningdek, ularni yollash usullariga moslashish qobiliyatiga ega ekanligini ta’kidlaydilar[2]. Ushbu o‘zgarishlarga samarali javob berish va ichki xavfsizlik sohasidagi ushbu yangi muammolarga qarshi turish uchun davlat keng qamrovli huquqiy va siyosiy vositalardan foydalanishi kerak. Ushbu vositalar mavjud tahdidlardan ishonchli himoyani ta’minlash uchun zarurdir. Garchi Markaziy Osiyo global kibertahdidlarning muhim manbai yoki global miqyosdagi xakerlar markazi sifatida ko‘p e’tirof etilmasada, mintaqa hukumatlari o‘z mamlakatlari boshqa davlatlarga qarshi kiberhujumlar uchun baza sifatida foydalanish imkoniyatlaridan xavotirda. Tez-tez uchraydigan terrorchilik tahdidlari va cheklangan ma’muriy, moddiy va texnologik resurslarning uyg‘unligi Markaziy Osiyo davlatlarini kiberterrorizmga nisbatan ayniqsa zaif holga keltirdi. Mintaqada xakerlar va veb-operatorlarning katta aholisi yashaydi, bu esa noyob milliy kiberidentifikatsiyalarning rivojlanishiga olib keldi. Iqtisodiyot va ijtimoiy infratuzilmaning turli tarmoqlarida faoliyat yurituvchi davlat boshqaruvi va vazirliklarning kollegial organlari, davlat qo‘mitalari va idoralari kiberterrorizmga qarshi kurashda hal qiluvchi rol o‘ynaydi. Vazirlik va idoralar tuzilmalarida monitoring tizimi segmentlarini nazorat qilish va boshqarish bo‘yicha bevosita boshqaruv organlari tashkil etilgani e’tiborga molik. Internet tarmog‘ining Milliy segmenti ustidan nazorat INFOCOM bozori sub’ektlari faoliyatini tartibga solish uchun mas’ul bo‘lgan idoralar va organlar tomonidan amalga oshiriladi. Shuni alohida ta’kidlash

[2] Marotta A, Madnick S. Convergence and divergence of regulatory compliance and cybersecurity.. Issues in Information Systems. 2021. mit.edu

kerakki, davlat organlari Internetning muayyan segmentlarini mustaqil ravishda nazorat qilib, yagona monitoring tizimiga birlashtirilgan, uning asosiy printsipi markazlashtirilgan markazdir. Prezident va Milliy xavfsizlik kengashining farmoyishlari hamda hukumat farmoyishlari muvofiq, davlatning barcha bo‘g‘inlarini samarali himoya qilish bo‘yicha ko‘plab davlat organlariga muhim vakolatlar va muhim vazifalar yuklatildi. Markaziy Osiyo davlatlari kiberxavfsizlikning global miqyosda e’tirof etilgan tamoyillari va standartlari bilan uyg‘unlashgan holda o‘z kibermakonini himoya qilishga mo‘ljallangan milliy kiberxavfsizlik bo‘yicha huquqiy tuzilmalarni shakllantirdi va yaratmoqda. Markaziy Osiyodagi ilg‘or kiberxavfsizlik qonunlari xalqaro kiberxavfsizlik normalari va ilg‘or tajribalarni amaliy qo‘llashga asoslangan. Binobarin, xalqaro va ichki jabhada diplomatik va boshqa tegishli choralar ko‘rish orqali Markaziy Osiyo davlatlari o‘zlarining xavfsizlik manfaatlari hamda global totuvlik va barqarorlik qadriyatlariga mos ravishda global kiberxavfsizlik boshqaruvini takomillashtirishga faol yordam bermoqda. Qirg‘izistondagi qonunchilik bazasi, 2009-yilda qabul qilingan “Terrorizmga qarshi kurash to‘g‘risida”gi qonunda ko‘rsatilganidek, terrorizmga qarshi kurash strategiyalarini va tegishli vakolatlarga ega bo‘lgan hokimiyat organlarini belgilaydi. Qonun, shuningdek, murakkab va kelishilgan terrorchilik aktlariga qarshi kurashda ishtirok etuvchi sub’ektlarning tashkiliy tuzilmasini ham belgilaydi. Bundan tashqari, u potentsial terrorchilik faoliyati haqida xabar berishni rag‘batlantiradigan qoidalarni o‘z ichiga oladi. Bundan farqli o‘laroq, Qozog‘istonda hozirda terrorizmning oldini olish va uning oqibatlarini yumshatishga qaratilgan keng qamrovli qonun mavjud enas. Mavjud konstitutsiyaviy va normativ-huquqiy hujjatlar terrorizm bilan bog‘liq muammolarni huquqiy boshqarishning mustahkam mexanizmi bo‘lib xizmat qilish uchun yetarli emas. Binobarin, ko‘rib chiqilayotgan masalalar ko‘lami, Qozog‘istonning ushbu sohadagi xalqaro majburiyatlaridan qat’i nazar, davlatlarning terrorizmga qarshi kurash bo‘yicha majburiyatlarini nizolarga yoki bajarmaslikka olib kelishi mumkin. O‘zbekistonning terrorizmga qarshi kurash to‘g‘risidagi qonunchiligida terrorizm og‘ir jinoyat sifatida belgilangan. Mamlakat huquqni muhofaza qilish organlari va terrorizmning oldini olish uchun mas’ul bo‘lgan boshqa davlat organlarining faoliyatini, shu jumladan potentsial terrorchilik faoliyati to‘g‘risida razvedka ma’lumotlarini to‘plashni, xavfsizlik choralarini (xavf ostida bo‘lgan hududlarni muhandislik va kinologik patrul qilish, texnik jihozlarni tekshirish kabi) amalga oshirishni boshqaradi. Terrorizmga qarshi maqsadlar), qurolli tezkor yuk va diplomatik himoyalangan yuklarning xavfsizligini baholash, nazorat-o‘tkazish punktlarini tashkil etish, terrorizmga qarshi kurashda davlat mansabdor shaxslarining o‘z vakolatlaridan foydalanishdagi roli va terrorizmga qarshi harakatlar uchun mol-mulkni rekvizitsiya qilish. Qozog‘istonning terrorizmga qarshi kurash

bo‘yicha asosiy qonunchiligi 2005-yildan beri amalda bo‘lgan “Ekstremistik faoliyatga qarshi kurashish to‘g‘risida”gi qonundir. Qonunda shaxsning shaxsiy hayotini ularning roziligisiz noqonuniy yozib olish yoki kuzatish bilan bog‘liq ikkita bo‘lim mavjud. Kompyuter tizimiga ruxsatsiz kirish qonunda belgilanganidek, jismoniy shaxsga yoki davlat yoki boshqa yuridik shaxsga zarar yetkazadigan “jiddiy zarar”ga olib kelgan taqdirda, jinoiy jazolar shu bobning boshqa qismida ko‘rsatilgan. Qozog‘iston Respublikasining terrorizmga qarshi kurash bo‘yicha qonuni keng qamrovli bo‘lib, terrorizmni keng qamrovli harakatlarni o‘z ichiga olgan holda belgilaydi, ularning ba’zilari odatda terrorizm deb hisoblanmaydi. O‘zbekistonning asosiy kiberjinoyatchilik va terrorizmga qarshi qonunlarida ham keng ta’riflar mavjud, garchi uning mustaqil aksilterror qonuni bu masalani hal qilishda to‘g‘ridan-to‘g‘ri bo‘lsada. Bundan farqli o‘laroq, Tojikiston va Qirg‘iziston ushbu hujjatning muqaddimasida ta’kidlanganidek, kiberterrorizmga qaratilgan qonunchilikka ega emas va bu atama tilga olinmaydi. Biroq, ular terrorizm bilan bog‘liq ayrim jinoyatlarni sodir etish uchun kompyuter texnologiyalaridan foydalanishni ko‘rib chiqadi. Hozirda ushbu mamlakatlar ma’lumotlar bazalarini yaratish va kiberjinoyatlar to‘g‘risidagi Vengriya konvensiyasini milliy huquqiy tizimlariga kiritish uchun materiallarni ko‘rib chiqish jarayonida va bu kiberterrorizmga qarshi qonunlarda jiddiy islohotlar o‘tkazish uchun alohida imkoniyatdir. 2003-yil 23-26-sentyabrda Bishkekda bo‘lib o‘tgan Xalqaro elektraloqa ittifoqining uchinchi Yevropa mintaqaviy yig‘ilishida kiberjinoyatchilikka qarshi kurash bo‘yicha keng qamrovli xalqaro hujjatni qabul qilish bo‘yicha mintaqaviy tashabbus ilgari surildi[3]. Uchrashuv yakunida davlatlarni kompyuter tarmoqlari orqali sodir etilayotgan og‘ir huquqbuzarliklar, jumladan, terrorizm harakatlarining oldini olish va ularga qarshi kurashish bo‘yicha xalqaro hamkorlikni mustahkamlash bo‘yicha ikki tomonlama va ko‘p tomonlama bitimlar hamda mexanizmlarni ishlab chiqishga chaqiruvchi rezolyutsiya qabul qilindi. Shuningdek, davlatlarga axborot almashinuvi, tegishli vakolatli organlar faoliyatini muvofiqlashtirish, vaqtincha ekstraditsiya qilish, kompyuter tarmoqlari doirasidagi jinoiy faoliyatni tergov qilish uchun texnik va huquqiy yordam ko‘rsatish orqali xalqaro va mintaqaviy hamkorlikni kengaytirish taklif etildi. Markaziy Osiyo davlatlarining ushbu tashabbuslarni nufuzli xalqaro hukumat va nohukumat tashkilotlari hamda asosiy hamkor-davlatlar bilan joriy munosabatlari nuqtai nazaridan ko‘rib chiqishga tayyorligi aholi va davlatlarga qarshi milliy strategiyalarda huquqiy sun’iy kompyuter tizimlarining samaradorligini oshirishga

[3] Al Asyari H. The Evolution of Cyberterrorism: Perspectives and Progress from The European Union and Association of Southeast Asian Nation. Jurnal Hukum Ius Quia Iustum. 2022. uii.ac.id

qaratilgan sa'y-harakatlarning samaradorligini belgilaydi. Xalqaro hamkorlik mustahkam huquqiy bazani yaratishda hal qiluvchi element hisoblanadi. Kiberfiribgarlik ko'plab alohida davlatlar uchun keng ko'lamli salbiy ta'sir ko'rsatishi mumkin bo'lgan jinoiy faoliyat turi ekanligini tan olish zarur. Bu borada mintaqaviy hukumatlararo aloqalar va hamkorlik muhim ahamiyat kasb etadi. Bir tomondan, Markaziy Osiyo davlatlari internetdan foydalanishga oid qoidalarni o'z ichiga olgan Axborotlashtirish sohasidagi faoliyatni tartibga solishning asosiy tamoyillari to'g'risidagi bitimni ratifikatsiya qilishdi. Boshqa tomondan, Mustaqil Davlatlar Hamdo'stligi axborot xavfsizligini ta'minlash bo'yicha hamkorlik to'g'risidagi bitimni qabul qildi. Jinoyatlarning virtual tarqalishining oldini olish uchun xalqaro miqyosda tan olingan usul va standartlardan foydalanishni nazarda tutgan holda kompyuter tarmoqlarida davlatlar va xususiy korxonalar xavfsizligini ta'minlash masalalari birinchi marta tashqi ishlar rahbarlari darajasida ko'tarildi. Tasdiqlangan kelishuv kiberjinoyatchilik oqibatlarining transmilliy tabiatining oldini olish va hal qilish uchun ham muhim ahamiyatga ega. Shunga qaramay, u birinchi navbatda global kelishuvni tashkil etadi va uni moslashtirish va tegishli davlatlarning mavjud yoki istiqbolli qonunchiligi doirasida amalga oshirish masalasi hal etilmagan. Bundan tashqari, Abu-Dabi deklaratsiyasida terrorizm va uning doirasidagi terrorchilik faoliyati masalalari ko'rib chiqildi. Markaziy Osiyodagi hamkorlikdagi sa'y-harakatlar Birlashgan Millatlar Tashkilotining tashabbuslarini qo'llab-quvvatlash va hamkorlik orqali yanada xavfsiz va farovon mintaqani qo'llab-quvvatlash uchun strategik yo'l xaritasi bo'lib xizmat qiluvchi "BMTning Markaziy Osiyo uchun Mintaqaviy dasturi" nizomini amalga oshirish orqali amalga oshirilishi mumkin. Markaziy Osiyo xavfsizligi va taraqqiyoti uchun muhim ahamiyatga ega bo'lgan mojarolarning oldini olish va zo'ravonlikka qarshi kurashish sohasidagi "Mintaqaviy dastur"ning asosiy maqsadi Markaziy Osiyo davlatlari o'rtasida do'stona munosabatlarni rivojlantirish va shu orqali muammolarni hal qilishda mintaqaviy yondashuvni ilgari surishdan iborat. Turli xil jamoalar (etnik, geografik va ijtimoiy) o'rtasida barqarorlikni ta'minlash va iqtisodiy aloqalarni kuchaytirish, ishonchni shakllantirish va xavfsizlikni ta'minlash. Yuqorida aytib o'tilgan masalalarni hisobga olgan holda shuni ta'kidlash mumkinki, yuqorida qayd etilgan qoidalarga muvofiq mintaqaviy qonun loyihasini ishlab chiqish qo'mitani tashkil etish uchun munosib loyiha bo'lib xizmat qilishi mumkin. Markaziy Osiyo davlatlarining kiberjinoyatchilikka qarshi kurashish va kiberterrorizmga qarshi kurashdagi hamkorligi e'tiborga molik ishdir. Bu kiberterrorizmga qarshi birgalikdagi sa'y-harakatlarga qaratilgan mintaqaviy nizomni yaratish va amalga oshirish uchun imkoniyat yaratadi. Buni milliy darajada kiberterrorizmga qarshi kurashish uchun shunga o'xshash qonunchilikka bo'lgan ehtiyojning e'tirof etilishi ham tasdiqlaydi.

Natijada, kiberterrorizmga qarshi kurashish uchun o‘zaro qonunlar qabul qilish imkoniyati ishonchli natijadir. Kiberjinoyat qonunlari va shartnomalari birinchi navbatda terrorizm va keng qamrovli ekspluatatsiyaga qarshi kurashga qaratilgan bo‘lsada, asosiy e’tibor kiberterrorizmning oldini olishga ham qaratilgan. Biroq, ular birinchi navbatda, faol oldini olish emas, balki jazoga qaratilgan. Tadqiqotlar va texnologiyalarni, xususan, zamonaviy mavjudlik bilan chambarchas bog‘liq bo‘lgan axborot asri va CISRIdan keyingi o‘zgarishlar kontekstida o‘z ichiga olish uchun moslashish talabi mavjud. Bu tarqoq qoidalarni ko‘rib chiqish va AQShning eksklyuziv bo‘lmagan kontseptsiyalari tomonidan shakllantirilgan rivojlanayotgan landshaftga moslashishga qaratilgan qonunchilik takliflariga ta’sir qilish uchun yetakchi kompaniyalar tomonidan ilg‘or tadqiqotlar o‘rtasida hamkorlikni osonlashtiradi. Huquqni muhofaza qilish organlari uchun kiberhuquq va tergov sohasida ixtisoslashgan mutaxassislar soni, texnik resurslarning mavjudligi yetarli emas va qoniqarli emas. Kiberhuquq bo‘yicha mutaxassislar ega bo‘lishi kerak bo‘lgan zarur bilimlar to‘g‘risida umumiy konsensus mavjud bo‘lsada, bu shaxslarning muhim qismi ish joyida kerakli ko‘nikmalarga ega emas. Bundan tashqari, ma’lumot almashish yoki treninglar va maslahatlar berishga tayyor bo‘lgan texnik tajribaga ega bo‘lgan tajribali mutaxassislar yetishmaydi. Aksariyat g‘arbiy mamlakatlarda bu sohada ixtisoslashgan oz sonli mutaxassislarga ega kiber tergov bo‘linmalari mavjud bo‘lsada, bu mamlakatlarning aksariyatida muhim voqealarni samarali hal qilish uchun zarur mutaxassislar yetishmaydi. Kiberterrorizmning asl mohiyati va jiddiyligini tan olish kiberterrorizmga oid qonunlarni qo‘llashda jiddiy muammo tug‘diradi. Kiberterrorizmning umume’tirof etilgan ta’rifining yo‘qligi mamlakatlar va xalqaro tashkilotlarga kiberterrorizmning turli holatlarini to‘g‘ri tasniflashni va kiberterrorizmga oid qonunlarni qachon qo‘llash kerakligini aniqlashni qiyinlashtiradi. Bundan tashqari, ayrim holatlar jinoiy xulq-atvor va terrorizm harakatlari o‘rtasidagi kulrang maydonni bosib o‘tishi mumkin, bu esa huquqni muhofaza qilish organlarini jinoiy qonunning yanada sodda choralari o‘rniga kiberterrorizmga qarshi sanksiyalarni qo‘llashda ikkilanishga olib keladi. Shunga qaramay, internetning keng qamrovini hisobga olgan holda, huquqni muhofaza qilish organlari ehtiyotkor bo‘lishda xato qilgani ma’qul. Z. Karp ta’kidlaganidek, potentsial terror aktlariga jiddiy munosabatda bo‘lmaslik uzoq vaqt davomida hujumni rejalashtirish va amalga oshirish imkoniyatini berishi mumkin. Kiberterrorizmning tabiati va namoyon bo‘lishi bilan bog‘liq noaniqlik turli mutaxassislar, jumladan professorlar V.Mikkolus va S.Uillis tomonidan e’tirof etilgan. Global miqyosda ushbu muammoni hal qilish uchun alohida kiberterrorizm konventsiyasi zarurligi bo‘yicha konsensus yo‘qligi ko‘rinishi[4]. Buning o‘rniga asosiy e’tibor an’anaviy

[4] ***Terrorist C. Countering Terrorist and Criminal Financing. api.taylorfrancis.com. . researchgate.net***

terrorizmga qarshi konventsiyalarni kengaytirish yoki qo‘shilishga qaratildi. Kiberterrorizmga oid qonun hujjatlari ustidan rasmiy nazoratga oid ayrim jihatlar, ular nazorati ostidagi nodavlat subyektlarning harakatlari uchun davlatlarning javobgarligi va ushbu muammolarni yanada samaraliroq hal qilish uchun alohida kiberterrorizm konventsiyasiga ehtiyoj borligi. Shuningdek, xalqaro kiberterrorizmni boshqarish bo‘yicha munozaralarning cheklanishini, davlatlar uchun kiberurushga va uning kuchayishi ehtimoliga qarshi kurashish zarurligini baholash, shuningdek, navigatsiya erkinligi, mutanosiblik va xavfsizlik kabi fundamental tamoyillarga muvofiq takliflar ishlab chiqish zarur. Xalqaro gumanitar huquq bo‘yicha farqlash printsipi. Bundan tashqari, raqamli qurollar va jinoiy ishlar o‘rtasidagi farq, shuningdek, kiber terrorizmning joriy ta’rifi bilan bog‘liq oqibatlarga oid aniqlik yo‘q.

Xulosa qilib aytish mumkinki, deyarli har bir davlat kiberterrorizmni tartibga solish orqali hal qilishga urinishgan. Biroq, eng keng tarqalgan tartibga solish shakllari, masalan, an’anaviy jinoiy kodekslarni oddiy qo‘llash yoki yangi noaniq va tushunarsiz kiberterrorizm qonunlarini yaratish turli muammolarni hal qilish uchun yetarli emas va fundamental huquqiy tamoyillarga mos kelmaydi. Shubhasiz, xalqlar o‘rtasida sezilarli madaniy, siyosiy, tarixiy va huquqiy tafovutlar mavjud va bu muammoning universal qo‘llaniladigan yechimi yo‘q. Shunga qaramay, ma’lum bir boshqaruv tamoyillari universaldir va ular kiberterrorizmga qarshi kurashni tartibga solish yoki qonunchilikni hal qilishda barcha mamlakatlar tomonidan amalga oshirilishi mumkinligi ta’kidlanadi. Global sa’y-harakatlar terrorizmning barcha shakllarini yo‘q qilishga qaratilgan bo‘lib, nisbatan kam sonli kiber hodisalar aniqlanmoqda. Qo‘shma Shtatlar boshchiligidagi ushbu tashabbus nafaqat kiberjinoyatchilikka qarshi kurashda, balki davlatlar o‘rtasidagi munosabatlarga ta’sir o‘tkazishda ham xalqaro hamkorlikni osonlashtirish salohiyatiga ega. Xorijiy hamkorlar bilan olib borilayotgan munozaralar va muzokaralarda axborot va telekommunikatsiya xavfsizligi mavzusi ko‘pincha potentsial tahdid sifatida Markaziy Osiyo mintaqasiga e’tibor qaratadi. Huquqni muhofaza qiluvchi idoralar o‘rtasida hamkorlik mavjud bo‘lsa-da, asosiy e’tibor transmilliy jinoyatchilikka qarshi kurashishga qaratilgan. Davra suhbatlari, seminarlar va amaliy mashg‘ulotlar ishtirokchilari so‘z erkinligi va boshqa inson huquqlarini himoya qilgan holda kiberterrorizmga qarshi kurashish zarurligidan doimiy ravishda norozilik bildiradilar. Markaziy Osiyoning ko‘pgina mamlakatlarida qonunlar va huquqiy jarayonlar kibermakondagi yutuqlar bilan hamohang emas, bu esa ularni noqonuniy faoliyat uchun, xususan, kiberterrorizmga qarshi kurashda qo‘llaniladigan zamonaviy texnologiyalarga qarshi kurashish uchun yetarlicha jihozlanmagan. Ushbu nomutanosiblik

xalqaro tashkilotlar tomonidan potentsial ravishda kapitallashtirilishi mumkin bo‘lgan bo‘shliqni yaratadi, ammo bu zaifliklardan foydalanish uchun joy qoldiradi.

FOYDALANILGAN ADABIYOTLAR:

1. Didenko AN. Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. Uniform Law Review. 2020. [HTML]

2. Marotta A, Madnick S. Convergence and divergence of regulatory compliance and cybersecurity.. Issues in Information Systems. 2021. mit.edu

3. Gulyamov SS, Khojiamonullokhonov AI. The concepts of" cyberterrorism" and the problems of its definition. Central Asian Academic Journal of Scientific Research. 2022;2(5):866-75. cyberleninka.ru

4. Al Asyari H. The Evolution of Cyberterrorism: Perspectives and Progress from The European Union and Association of Southeast Asian Nation. Jurnal Hukum Ius Quia Iustum. 2022. uii.ac.id

5. Sharifovna YN. The characteristics of cyberterrorism. Asian Journal of Research in Social Sciences and Humanities. 2022;12(11):21-4. scienceweb.uz

6. Citaristi I. Organization For Security And Co-Operation In Europe—OSCE. InThe Europa Directory of International Organizations 2022 2022 Jul 28 (pp. 704-717). Routledge. [HTML]

7. Canton H. Organization for Security and Co-Operation in Europe—OSCE. InThe Europa Directory of International Organizations 2021 2021 Jul 28 (pp. 688-702). Routledge. [HTML]

8. Terrorist C. Countering Terrorist and Criminal Financing. api.taylorfrancis.com. . researchgate.net

9. Saif I, Khouri R. The Relationship between Economic Interdependence and Conflict Prevention: An Institutional Perspective. 2021. erf.org.eg

10. Wayne EA. Imagine Peace: Connecting Global Solutions on Reconciliation with an Afghanistan Ready for Peace. 2022. [HTML]