ISSN 2181-3187

"RAQAMLI HUQUQBUZARLIKLARNING JINOIY-HUQUQIY TAHLILI VA HIMOYA CHORALARI"

Zulayxo Usanova Turdimurod qizi
Termiz davlat universiteti Yuridik fakulteti 1-bosqich talabasi
Elektron pochta: ongboyevazulayho@gmail.com

Gulnoza Jumayeva Sodiq qizi
Termiz davlat universiteti Yuridik fakulteti 1-bosqich talabasi
Elektron pochta: lucy0060606@gmail.com

O`qituvchi: Adham Avliyoqulov Alisherovich

Annotatsiya: Ushbu maqola kiber jinoyatlarning huquqiy jihatlarini xalqaro normalar va turli davlatlarning qonunchilik tajribasi asosida o‘rganadi. Budapesht konvensiyasi, Birlashgan Millatlar Tashkiloti hujjatlari va xorijiy huquqiy amaliyot doirasida kiber firibgarlik, shaxsiy ma’lumotlarning noqonuniy qo‘lga kiritilishi va xakerlik hujumlarining huquqiy bahosi tahlil qilinadi.Bundan tashqari, xalqaro tashkilotlar va huquqni muhofaza qilish institutlarining kiber jinoyatlarga qarshi kurashdagi o‘rni yoritilib, qonunchilikni takomillashtirish bo‘yicha takliflar ilgari suriladi.

Kalit so‘zlar:Raqamli huquqbuzarliklar, taditranschegaraviy kiber huquq, kiber suverenitet va huquqiy yurisdiksiya,raqamli aktivlar va shaxsiy ma’lumotlar himoyasi,

kiber jinoyatlarga qarshi xalqaro konvensiyalar, kiber forensika va elektron dalillar tahlili,raqamli moliyaviy jinoyatlar va kiber iqtisodiy xavfsizlik, global kiber xavfsizlik arxitekturasi.

Kirish

ISSN 2181-3187

Axborot texnologiyalarining jadal rivojlanishi zamonaviy jamiyatning barcha sohalariga chuqur ta’sir ko‘rsatib, yangi huquqiy muammolarni keltirib chiqarmoqda. Raqamli makon kengaygani sari kiber jinoyatlar ham o‘sib bormoqda. Ushbu jinoyatlar orasida moliyaviy firibgarlik, shaxsiy ma’lumotlarning noqonuniy qo‘lga kiritilishi, intellektual mulk huquqlarining buzilishi, zararli dasturlar tarqatish va kompyuter tizimlariga ruxsatsiz kirish kabi huquqbuzarliklar mavjud bo‘lib, ular nafaqat jismoniy va yuridik shaxslarga, balki davlatlarning axborot xavfsizligiga ham tahdid solmoqda.

Kiber jinoyatlar transchegaraviy xarakterga ega bo‘lib, jinoyatchilar internet texnologiyalaridan foydalanib, turli mamlakatlardagi qurbonlarga zarar yetkazishi mumkin. Shu sababli, bunday jinoyatlarga qarshi samarali kurashish xalqaro hamkorlikni talab qiladi. Yagona davlat doirasida qabul qilingan qonunchilik ushbu jinoyatlarning oldini olish va ularni jazolash uchun yetarli bo‘lmasligi mumkin. Bu esa xalqaro huquqiy mexanizmlarni ishlab chiqish va ularni takomillashtirish zaruratini yuzaga keltiradi.

Kiber jinoyatlarga qarshi kurashda eng muhim xalqaro hujjatlardan biri Budapesht konvensiyasi bo‘lib, u kiber jinoyatlarning ta’rifini belgilaydi, ularni jinoyat sifatida tasniflaydi va davlatlar o‘rtasida hamkorlik mexanizmlarini shakllantiradi. Ushbu konvensiya xalqaro tergov hamkorligini mustahkamlash, elektron dalillarni yig‘ish va jinoyatchilarni ekstraditsiya qilish bo‘yicha huquqiy asos yaratadi. Bundan tashqari, Birlashgan Millatlar Tashkiloti rezolyutsiyalari, Interpol va Europol tomonidan ishlab chiqilgan xalqaro tavsiyalar ham kiber jinoyatlarga qarshi kurashish strategiyalarini belgilashda muhim ahamiyat kasb etadi.

Shunga qaramay, zamonaviy texnologiyalarning tezkor rivojlanishi kiber jinoyatlarning yangi shakllarini vujudga keltirmoqda, bu esa mavjud xalqaro huquqiy me’yorlarning samaradorligini pasaytirishi mumkin. Raqamli jinoyatlar bilan bog‘liq huquqiy bo‘shliqlar ayrim davlatlarda hali to‘liq bartaraf etilmagan bo‘lib, bu esa jinoyatchilarga ma’lum darajada huquqiy imkoniyatlar yaratib bermoqda. Shu sababli,

ISSN 2181-3187

kiber jinoyatlarga qarshi kurashish strategiyalarini doimiy ravishda yangilash va xalqaro hamkorlikni yanada rivojlantirish zarur.

Ushbu maqola kiber jinoyatlarning huquqiy asoslarini tahlil qilish, xalqaro huquqiy me'yorlarni o'rganish va ushbu jinoyatlarga qarshi samarali mexanizmlarni taklif etish maqsadida tayyorlangan. Maqolada kiber jinoyatlarning huquqiy ta'rifi va tasnifi, Budapesht konvensiyasining ahamiyati, xalqaro tashkilotlarning roli, davlatlar darajasida kiber xavfsizlikni ta'minlash choralari, raqamli kriminalistika va huquqni muhofaza qilish institutlari faoliyati hamda kiber jinoyatlarga oid qonunchilikni takomillashtirish bo'yicha huquqiy takliflar ilmiy jihatdan tahlil qilinadi.

Maqolada xalqaro huquqiy manbalar, xalqaro tashkilotlarning tavsiyalari hamda turli mamlakatlarning qonunchilik tajribasi asosida komparativ-huquqiy tahlil, normativ-huquqiy tahlil, empirik yondashuv va tizimli-huquqiy tahlil kabi ilmiy metodlardan foydalanilgan. Ushbu yondashuvlar orqali kiber jinoyatlarga oid xalqaro va milliy huquqiy me'yorlarning samaradorligi baholanadi va huquqiy islohotlar bo'yicha tavsiyalar ilgari suriladi.

Mazkur maqola natijalari xalqaro huquqshunoslar, huquqni muhofaza qilish organlari, davlat siyosatini ishlab chiquvchilar va kiber xavfsizlik sohasi mutaxassislari uchun amaliy ahamiyatga ega bo'lib, xalqaro miqyosda samarali huquqiy mexanizmlar yaratish bo'yicha tavsiyalar ishlab chiqishga xizmat qiladi.

Kiber jinoyatlar zamonaviy global huquqiy tizim uchun eng dolzarb muammolardan biriga aylandi. Axborot texnologiyalarining jadal rivojlanishi natijasida nafaqat iqtisodiy va ijtimoiy munosabatlar, balki huquqiy munosabatlar ham tubdan o'zgarib, yangi xavfsizlik tahdidlari paydo bo'ldi. Kiber jinoyatlar an'anaviy jinoyatlardan tubdan farq qiladi, chunki ular o'z mohiyatiga ko'ra transchegaraviy, anonim va murakkab texnologik vositalardan foydalangan holda amalga oshiriladi. Interpol va Europolning 2024-yilgi hisobotlariga ko'ra, global miqyosda kiber jinoyatlar soni 18% ga oshgan, bu esa ushbu jinoyatlar bilan kurashish bo'yicha

ISSN 2181-3187

xalqaro hamkorlik va huquqiy normalarni takomillashtirish zarurligini yana bir bor tasdiqlaydi.

Xalqaro huquqiy normalar kiber jinoyatlarni ikkita asosiy guruhga ajratadi. Birinchisi – axborot tizimlariga qarshi jinoyatlar, ya'ni, texnologik vositalarning buzilishi yoki noqonuniy ishlatilishi bilan bog'liq huquqbuzarliklar. Bu turdagi jinoyatlarga xakerlik hujumlari, zararli dasturlar yaratish va tarqatish, DDoS (Distributed Denial of Service) hujumlar va kompyuter firibgarligi kiradi. Ikkinchi guruh esa axborot tizimlari orqali sodir etiladigan jinoyatlar bo'lib, bunda kiber makon jinoyat sodir etish vositasi sifatida ishlatiladi. Bu turdagi jinoyatlarga moliyaviy firibgarlik, shaxsiy ma'lumotlarni o'g'irlash, onlayn tovlamachilik, noqonuniy kontent tarqatish va intellektual mulk huquqlarining buzilishi kiradi.

So'nggi yillardagi statistik ma'lumotlar ushbu jinoyatlarning o'sish tendensiyasini tasdiqlaydi. Europolning 2024-yilgi ma'lumotlariga ko'ra, 2023-yilda kiber firibgarlik global kiber jinoyatlarning 40% ini tashkil etgan, bu esa eng keng tarqalgan jinoyat turi ekanligini ko'rsatadi. Interpolning hisobotida esa 2023-yilda shaxsiy ma'lumotlarning noqonuniy qo'lga kiritilishi 25% ga oshgani va global miqyosda 5 milliarddan ortiq ma'lumotlar o'g'irlangani qayd etilgan. Birlashgan Millatlar Tashkiloti ma'lumotlariga ko'ra, DDoS (Distributed Denial of Service) hujumlar soni 2023-yilda 15% ga oshib, davlat idoralari va yirik korxonalarga katta zarar yetkazgan. Ushbu ko'rsatkichlar xalqaro huquqiy me'yorlarni takomillashtirish zaruratini yanada kuchaytiradi.

Kiber jinoyatlarga qarshi kurashish bo'yicha eng muhim xalqaro-huquqiy hujjatlardan biri Budapesht konvensiyasi hisoblanadi. Ushbu konvensiya kiber jinoyatlarni aniqlash, oldini olish va ularga qarshi kurashish bo'yicha xalqaro huquqiy mexanizmlarni belgilaydi. 2024-yil holatiga ko'ra, Budapesht konvensiyasiga 70 dan ortiq davlat qo'shilgan, bu esa global kiber xavfsizlik hamkorligining ortib borayotganini ko'rsatadi. Ushbu konvensiya kiber jinoyatlarni yagona xalqaro tushunchalar asosida tasniflash, davlatlar o'rtasida huquqiy yordam mexanizmini

ISSN 2181-3187

yaratish, tergov va ayblanuvchilarning ekstraditsiyasini soddalashtirish, elektron dalillarni qonuniy asosda yig‘ish va ulardan foydalanish kabi tamoyillarni o‘z ichiga oladi.

Bundan tashqari,Birlashgan Millatlar Tashkiloti, Interpol va Europol ham kiber jinoyatlarga qarshi kurashishda muhim rol o‘ynaydi.Birlashgan Millatlar Tashkiloti 2023-yilda "Kiber jinoyatlarga qarshi global strategiya"ni qabul qildi, bu esa xalqaro huquqiy hamkorlikni mustahkamlashga xizmat qilmoqda. Interpol 2023-yilda kiber jinoyatlarga qarshi 60 dan ortiq xalqaro operatsiyalarni muvofiqlashtirdi va 3000 dan ortiq kiber jinoyatchini qo‘lga oldi. Europol esa 2024-yilda Yevropada moliyaviy kiber jinoyatlarga qarshi kurash bo‘yicha yangi qoidalarni joriy qildi, natijada kiber firibgarlik darajasi 12% ga kamaydi.

Har bir davlat kiber jinoyatlarga qarshi o‘ziga xos qonunchilik modelini ishlab chiqqan. Amerika Qo’shma Shtatlarida CFAA (Computer Fraud and Abuse Act) va Patriot Akti (USA PATRIOT Act) qonunlari kiber jinoyatlarga qarshi qat’iy choralarni nazarda tutadi. 2023-yilda Amerika Qo’shma Shtatlari hukumati "Kiber Jinoyatlarga qarshi maxsus federal dastur"ni yo‘lga qo‘ydi, bu esa davlat va xususiy sektor hamkorligini kuchaytirdi. Yevropa Ittifoqi GDPR asosida shaxsiy ma’lumotlarni himoya qilish bo‘yicha qat’iy choralar qabul qilgan bo‘lib, 2024-yilda esa "Kiber Xavfsizlik Akti" yangilandi, bu esa xalqaro huquqiy hamkorlikni mustahkamlashga qaratilgan. Osiyo davlatlari, jumladan Xitoy, Yaponiya va Janubiy Koreya, kiber jinoyatlarga qarshi qat’iy qonunlarga ega bo‘lib, Xitoy 2023-yilda raqamli infratuzilmalar himoyasini kuchaytiruvchi yangi qonunlarni qabul qildi, Janubiy Koreya esa sanksiyalarni kuchaytirish orqali firibgarlikka qarshi kurash strategiyasini takomillashtirdi.

Mustaqil Davlatlar Hamdo'stligi davlatlari ham ushbu sohada faoliyat olib bormoqda. Rossiya, Qozog‘iston va O‘zbekiston o‘z milliy qonunchiligini shakllantirgan bo‘lib, O‘zbekiston 2024-yilda "Axborot xavfsizligi strategiyasi"ni qabul qildi, bu esa davlat sektoridagi raqamli infratuzilmalarni himoya qilishga

ISSN 2181-3187

yo‘naltirilgan. Kiber jinoyatlar global muammo bo‘lgani sababli, har bir davlatning o‘z qonunchilik tizimi mavjud bo‘lsa-da, xalqaro huquqiy normalarga moslashish muhim. Shu sababli, Budapesht konvensiyasi asosida xalqaro huquqiy tizimlarni uyg‘unlashtirish va davlatlar o‘rtasidagi hamkorlikni kuchaytirish kiber jinoyatlarga qarshi kurashish samaradorligini oshiradi.

Axborot texnologiyalarining jadal rivojlanishi bilan bog‘liq holda, kiber jinoyatlar nafaqat davlatlar xavfsizligiga, balki global iqtisodiy barqarorlik va shaxsiy ma’lumotlarning daxlsizligiga ham jiddiy tahdid tug‘dirmoqda. Interpol, Europol va Birlashgan Millatlar Tashkilotining 2024-yilgi hisobotlariga ko‘ra, oxirgi besh yil ichida kiber jinoyatlar global miqyosda 3 baravarga oshgan. Ushbu raqamlar xalqaro huquqiy mexanizmlarni takomillashtirish zarurligini yana bir bor tasdiqlaydi. Raqamli jinoyatlar xalqaro huquqiy jihatdan Budapesht konvensiyasi, Yevropa Ittifoqining Umumiy Ma’lumotlarni Himoya Qoidalari va Birlashgan Millatlar Tashkilotining "Kiber Jinoyatlarga qarshi strategiyasi" kabi hujjatlar bilan tartibga solinadi. Biroq, kiber jinoyatlar doimiy ravishda rivojlanib, huquqiy tizimlarni yangi xavf-xatarlarga moslashtirishni talab qilmoqda. Xalqaro huquqiy me’yorlar raqamli jinoyatlarni uch asosiy toifaga ajratadi: moliyaviy kiber jinoyatlar va firibgarlik, shaxsiy ma’lumotlarning noqonuniy qo‘lga kiritilishi va tarqatilishi hamda xakerlik hujumlari va kiber terrorizm.

Kiber firibgarlik raqamli infratuzilmalar, moliyaviy tizimlar va internet platformalar orqali amalga oshiriladigan iqtisodiy jinoyatlar bo‘lib, soxta tranzaksiyalar, noqonuniy pul o‘tkazmalari va shaxsiy identifikatsiya ma’lumotlaridan foydalanish orqali moddiy manfaat olish kabi shakllarga ega. Amerika Qo‘shma Shtatlarining Federal Qidiruv Byurosi ma’lumotlariga ko‘ra, 2023-yilda kiber firibgarlik natijasida global iqtisodiyotga yetkazilgan zarar 1,5 trillion AQSh dollaridan oshgan. Bu esa xalqaro moliyaviy xavfsizlikka jiddiy tahdid tug‘diradi. Yevropa Ittifoqining 2024-yilgi "Moliyaviy Jinoyatlarga qarshi kurash strategiyasi" esa global bank tizimlari va moliyaviy institutlarning kiber firibgarlikka qarshi

ISSN 2181-3187

himoyasini kuchaytirishni nazarda tutadi. Budapesht konvensiyasi kiber firibgarlikni xalqaro jinoyat sifatida tasniflaydi va davlatlar o‘rtasida huquqiy hamkorlikni mustahkamlashni talab qiladi. Moliyaviy harakatlar bo‘yicha ishchi guruhi esa xalqaro moliyaviy tranzaksiyalar monitoringini kuchaytirish mexanizmlarini ishlab chiqmoqda.

Raqamli davrda shaxsiy ma’lumotlarning himoyasi global xavfsizlikning asosiy masalalaridan biriga aylandi Birlashgan Millatlar Tashkilotining 2024-yilgi kiber xavfsizlik bo‘yicha hisobotiga ko‘ra, so‘nggi yilda 5 milliarddan ortiq shaxsiy ma’lumot noqonuniy tarqatilgan yoki o‘g‘irlangan. Yevropa Ittifoqining Umumiy Ma’lumotlarni Himoya Qoidalari ushbu muammoni hal qilish uchun qabul qilingan eng qat’iy xalqaro huquqiy hujjatlardan biri bo‘lib, u shaxsiy ma’lumotlarni himoya qilish, noqonuniy uzatilishini cheklash va korxonalarning javobgarlik mexanizmlarini kuchaytirishni nazarda tutadi. Budapesht konvensiyasining 8-moddasi shaxsiy ma’lumotlarni noqonuniy olish va tarqatish xalqaro jinoyat ekanligini belgilaydi va ushbu jinoyatlarga qarshi kurashda davlatlar o‘rtasidagi hamkorlikni kuchaytirishni talab qiladi.

Xakerlik hujumlari davlat va xususiy sektor infratuzilmalariga qaratilgan texnologik jinoyatlardan biri bo‘lib, bu ma’lumotlarni buzish, maxfiy hujjatlarni o‘g‘irlash va muhim tizimlarni ishdan chiqarish orqali amalga oshiriladi. Interpol va Birlashgan Millatlar Tashkilotining 2024-yilgi statistik ma’lumotlariga ko‘ra, 2023-yilda davlat infratuzilmalari va yirik korporatsiyalarga qilingan xakerlik hujumlari soni 20% ga oshgan. Xakerlik hujumlarining eng xavfli shakllaridan biri bu kiber terrorizm bo‘lib, davlat infratuzilmalariga qaratilgan keng ko‘lamli texnologik tahdidlarni o‘z ichiga oladi. Birlashgan Millatlar Tashkilotining 2024-yilda qabul qilingan Kiber Jinoyatlarga qarshi strategiyasi terrorchilik guruhlarining kiber hujumlari global xavfsizlikka jiddiy tahdid solayotganini ta’kidlaydi. Budapesht konvensiyasining 2-moddasi ruxsatsiz tizimlarga kirish va davlat infratuzilmalariga zarar yetkazishni xalqaro jinoyat deb belgilaydi. Yevropa Ittifoqining 2024-yilda tasdiqlangan Yevropa

ISSN 2181-3187

Kiber Xavfsizlik Direktivasida esa barcha a’zo davlatlar xakerlik jinoyatlariga qarshi kuchaytirilgan huquqiy mexanizmlar joriy etishi kerakligi belgilangan.

Raqamli jinoyatlar zamonaviy global huquqiy tizim oldida turgan eng dolzarb muammolardan biri bo‘lib, Budapesht konvensiyasi, Yevropa Ittifoqi reglamentlari va Birlashgan Millatlar Tashkiloti strategiyalari ushbu jinoyatlarga qarshi samarali choralarni ishlab chiqmoqda. Biroq, zamonaviy texnologik taraqqiyot bilan huquqiy normalarni doimiy ravishda yangilash va xalqaro hamkorlikni yanada mustahkamlash zarur. Global miqyosda yangi qonunlar ishlab chiqish va amaldagi huquqiy normalarni modernizatsiya qilish kiber jinoyatlarga qarshi kurash samaradorligini oshirishning asosiy shartidir.

Kiber jinoyatlar transchegaraviy xarakterga ega bo‘lib, ularga qarshi samarali kurashish xalqaro hamkorlik, mustahkam qonunchilik va ilg‘or texnologiyalarga asoslangan xavfsizlik choralari bilan amalga oshirilishi lozim. Hozirgi davrda kiber jinoyatchilik faqatgina individual shaxslar yoki kompaniyalarga emas, balki butun davlatlarning iqtisodiy va axborot infratuzilmasiga ham tahdid solmoqda. Shu sababli, kiber jinoyatlarga qarshi global va milliy darajadagi huquqiy choralarni takomillashtirish hamda zamonaviy texnologik xavfsizlik mexanizmlarini ishlab chiqish dolzarb ahamiyat kasb etadi.

Kiber jinoyatlarga qarshi samarali kurashishning asosiy yo‘nalishlaridan biri xalqaro tashkilotlarning roli va ularning huquqiy vakolatlarini mustahkamlashdir. INTERPOL, Europol va Birlashgan Millatlar Tashkiloti (BMT) kiber jinoyatchilikka qarshi global miqyosda kurashuvchi asosiy tashkilotlar bo‘lib, ular davlatlararo hamkorlikni ta’minlash, tergov jarayonlarini muvofiqlashtirish va kiber jinoyatchilarning transchegaraviy ekstraditsiya jarayonlarini soddalashtirishda muhim rol o‘ynaydi. Masalan, INTERPOL 2023-yilda xalqaro kiber jinoyatchilikka qarshi 60 dan ortiq maxsus operatsiyalarni muvofiqlashtirib, 3000 dan ortiq kiber jinoyatchini qo‘lga oldi. Europol esa moliyaviy kiber firibgarlikka qarshi kurash bo‘yicha 2024-yilga mo‘ljallangan yangi monitoring tizimini joriy qildi. Ushbu tashkilotlarning

ISSN 2181-3187

imkoniyatlarini kengaytirish va ularning tergov faoliyatini tezkorlashtirish global kiber xavfsizlikni ta’minlashda muhim o‘rin tutadi.

Davlat darajasida kiber xavfsizlikni ta’minlash uchun har bir mamlakat o‘z qonunchiligini mustahkamlashi va xalqaro normalarga moslashtirishi zarur. Kiber jinoyatlar xalqaro miqyosda tartibga solinayotgan bo‘lsa-da, ayrim mamlakatlarning qonunchiligi ushbu jinoyatlarga nisbatan yetarlicha qat’iy emas. Masalan, Yevropa Ittifoqining Umumiy Ma’lumotlarni Himoya Qoidalari (GDPR) shaxsiy ma’lumotlarning maxfiyligini ta’minlash bo‘yicha eng qat’iy xalqaro hujjatlardan biri hisoblanadi, ammo hali ham ko‘plab davlatlarda shaxsiy ma’lumotlarni noqonuniy foydalanishning oldini oluvchi mexanizmlar yetarlicha rivojlanmagan. Shu sababli, davlatlar o‘z milliy qonunchiliklarini Budapesht konvensiyasi va xalqaro tavsiyalarga moslashtirib borishlari lozim.

Raqamli kriminalistika va huquqni muhofaza qilish institutlarining faoliyati ham kiber jinoyatlarga qarshi samarali kurashning ajralmas qismidir. Zamonaviy tergov usullari kiber jinoyatchilikning murakkab xususiyatiga moslashishi kerak. Sun’iy intellekt, blokcheyn texnologiyalaridan foydalangan holda moliyaviy jinoyatlarni kuzatish va kiber hujumlarni real vaqt rejimida kuzatish texnologik taraqqiyotning eng samarali yo‘nalishlaridan biridir. Masalan, AQSh Federal qidiruv byurosi 2023-yilda sun’iy intellekt yordamida kiber jinoyatchilik bilan bog‘liq 150 dan ortiq hujumning oldini olgan. Shuning uchun, davlatlar raqamli kriminalistika tizimlariga sarmoya kiritishi va tergov usullarini texnologik jihatdan takomillashtirishi zarur.

Kiber jinoyatlarga qarshi samarali kurashish uchun xalqaro hamkorlikning rivojlanishi muhim ahamiyatga ega. Ko‘plab kiber jinoyatlar bir davlat hududida sodir bo‘lib, boshqa davlat hududida tugallanadi, bu esa xalqaro tergov jarayonlarini murakkablashtiradi. Budapesht konvensiyasining asosiy maqsadlaridan biri shundan iboratki, davlatlar o‘zaro ma’lumot almashinuvini kuchaytirib, kiber jinoyatchilarning javobgarlikka tortilishini ta’minlashlari kerak. Shuningdek, ekstraditsiya

jarayonlarining tezkor va samarali amalga oshirilishi jinoyatchilarning jazodan qochib qutulishining oldini oladi.

Texnologik xavfsizlikni oshirish strategiyalari ham kiber jinoyatlarga qarshi huquqiy choralar bilan birgalikda olib borilishi lozim. Axborot tizimlarini mustahkamlash, xodimlarning kiber xavfsizlik bo‘yicha malakasini oshirish va xususiy sektor bilan hamkorlik qilish bugungi kunda global kiber xavfsizlikning ajralmas qismi hisoblanadi. Kiber hujumlarning oldini olish bo‘yicha sun’iy intellekt asosida ishlovchi tizimlar joriy etilmoqda va davlat organlari hamda xususiy kompaniyalar o‘rtasida kiber xavfsizlik bo‘yicha hamkorlik kengaymoqda.

Xulosa

Xulosa qilib aytganda, kiber jinoyatlar zamonaviy dunyoda davlat suvereniteti, iqtisodiy barqarorlik va shaxsiy xavfsizlikka jiddiy tahdid tug‘dirayotgan global muammo hisoblanadi. Ularning transchegaraviy tabiati milliy qonunchilik doirasida samarali nazoratni imkonsiz qiladi. Shu sababli, yagona xalqaro yondashuv va huquqiy mexanizmlar ishlab chiqilishi zarur.Ushbu muammoga qarshi kurashish uchun BMT doirasida "Kiber Jinoyatlarga Qarshi Xalqaro Tribunal" tashkil etish samarali yechim bo‘lishi mumkin. Mazkur maxsus sud organi transchegaraviy kiber jinoyatlarni tergov qilish, xalqaro huquqiy hamkorlikni rivojlantirish hamda jinoyatchilarning jazodan qochish ehtimolini kamaytirishga qaratilgan bo‘lishi lozim. Kiber xavfsizlikni ta’minlash uchun xalqaro hamkorlikni mustahkamlash, sun’iy intellekt va ilg‘or texnologiyalarni huquqiy tizimga integratsiya qilish shart. Jazo muqarrarligi prinsipini global darajada ta’minlamasdan, kiber jinoyatlarga qarshi kurashda muvaffaqiyatga erishib bo‘lmaydi.

Foydalanilgan adabiyotlar.

1. **Convention on Cybercrime (Budapest Convention, 2001).** Council of Europe. – URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (date of reference: 15.03.2024).

2. **United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime.** United Nations, 2023. – URL: https://www.unodc.org/documents/cybercrime/study (date of reference: 10.03.2024).

3. **General Data Protection Regulation (GDPR, 2016).** Official Journal of the European Union, L 119. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (date of reference: 12.03.2024).

4. **Computer Fraud and Abuse Act (CFAA, 1986).** United States Congress. – URL: https://www.govinfo.gov/content/pkg/USCODE-2023-title18/pdf/USCODE-2023-title18.pdf (date of reference: 14.03.2024).

5. **European Cybersecurity Act (2024).** European Commission. – URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity (date of reference: 11.03.2024).

6. **China's Cybersecurity Law (2017, amended in 2023).** National People's Congress of China. – URL: http://www.npc.gov.cn/englishnpc/cyberlaw (date of reference: 09.03.2024).

7. **INTERPOL Global Cybercrime Report (2024).** International Criminal Police Organization (INTERPOL). – URL: https://www.Interpol.int/en/Crimes/Cybercrime (date of reference: 13.03.2024).

8. **Europol Internet Organised Crime Threat Assessment (IOCTA, 2024).** Europol. – URL: https://www.europol.europa.eu/cybercrime (date of reference: 08.03.2024).

9. **Federal Bureau of Investigation (FBI). Internet Crime Report (2023).** United States Department of Justice. – URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (date of reference: 10.03.2024).

ISSN 2181-3187

10. **Clough, J. (2015). Principles of Cybercrime.** Cambridge University Press. – 288 p.