

SCIENCEZONE

ONLINE SCIENTIFIC
CONFERENCES

Conference

On Legal Science

No.1 (2)

2024

<i>Abdihakimov Farhod Zafar o'g'li</i> ELEKTRON TIJORATDA SOTUVCHI MANFAATLARINI HUQUQIY HIMOYA QILISH	4-10
<i>Olimjonova Hulkar To'lqin qizi</i> SUG'URTA KOMPANIYALARI FOND BOZORIDA INSTITUTSIONAL INVESTOR SIFATIDA	11-15
<i>Razzaqova E'zoza Yusup qizi</i> ISLOM MOLIYASIDA MUSHOKARA SHERIKCHILIK BITIMINING TUTGAN O'RNI	16-22
<i>Xudayqulova Nodira Qo'ldoshjonovna</i> HISSADORLIKKA ASOSLANGAN KRAUDFANDING FAOLIYATIDA INVESTOR HUQUQLARI HIMOYASI VA QIMMATLI QOG'OZLAR AYLANISHIDA VUJUDGA KELADIGAN MUAMMOLAR	23-28
<i>Salimov Islombek Bobir o'g'li</i> O'ZBEKISTONDA ELEKTRON TIJORAT: SOHAGA OID MUAMMOLAR VA ULARGA YECHIMLAR	29-34
<i>Odilov Nozimjon Jumanazar o'g'li</i> UCHINCHI TOMON PROVAYDERLARINING MIJOZ MOLIYAVIY MA'LUMOTLARIGA KIRISHINING HUQUQIY ASOSLARI	35-39
<i>Xudoyorov Fayzullo Sayfulla o'g'li</i> MUSHARAKA VA MUDARABAH INTEGRATSIYASI: O'ZBEKISTONNING UMUMIY SHERIKLIK KELISHUVI DOIRASIDA ISLOMIY MOLIYA VOSITALARI	40-46
<i>G'ulomov Shohruh Islomjon o'g'li</i> TRANSMILLIY KORPORATSIYALAR TOMONIDAN SOLIQ MILLIY BAZASI YEMIRLISHINING OLDINI OLIH USULLARI	47-50
<i>Shaimardanova Dilafruz</i> ETHICAL ASPECTS OF DIGITAL ESTATE MANAGEMENT: CONFIDENTIALITY, RESPECT FOR WILL, AND NORMS OF INHERITANCE LAW	51-58
<i>Xonzodabegim Raxmatova Utkir qizi</i> KIBER HUQUQ UCHUN YURISDIKSIYANI VA XALQARO HAMKORLIKNI TARTIBGA SOLINISHI	59-73
<i>Sabohat Abdullayeva</i> BLOKCHEYN ASOSIDAGI RAQAMLI SUD EKSPERTIZASI VOSITALARI	74-84

Asal Juraeva

CHOICE OF SUBSTANTIVE AND PROCEDURAL LAW IN INTERNATIONAL
COMMERCIAL ARBITRATION85-91

Xudoyberdiyev Nuriddin Olloberdi o'g'li

KIBERHUQUQDA YURIDIKSIYA MASALALARI – ONLAYN MUHITDA QAYSI
DAVLAT QONUNCHILIGI QO'LLANILADI? 92-103

Rabbimov Shohruh

RAQAMLI ASRDA FUQAROLIK ERKINLIKLARI VA ULARNI
MUVOZANATLASH 104-112

Abbosjon Olimov

KIBER JINOYATLARNI TERGOV QILISH BILAN BOG'LIQ XALQARO ISO
STANDARTLAR VA ULARNI OZBEKISTON QONUNCHILIGIGA
INTEGRATSIYALASH 112-125

Mirzakarimova Dilafruz

KIBERXAVFSIZLIK VA YURISDIKSIYA CHEGARALARINI BELGILASH
MUAMMOLARI VA ULARNING YECHIMLARI 126-134

Normurodova Behro'za Xolmo'minovna

RAQAMLI OCHIQ MANBALAR ORQALI DALILLAR TO'PLASH VA TERGOV
QILISHDA SUN'IY INTELLEKTDAN FOYDALANISH..... 135-143

Gulomov Shokhrukh Islomjon ugli

REGULATORY FRAMEWORKS FOR METAVERSE PLATFORMS: CHALLENGES
AND OPPORTUNITIES..... 144-151

O'razbayev Laziz Shuhrat o'g'li

MAMLAKATIMIZDA RAQAMLI INFRATUZILMALARNI RIVOJLANTIRISH UCHUN
OLIB BORILAYOTGAN CHORA-TADBIRLARNING AHAMIYATI 152-158

Olimjonova Hulkar To'lqin qizi

MOLIYAVIY VOSITACHILAR ORASIDA SUG'URTA KOMPANIYALARINING
TUTGAN O'RNI 159-162

KIBERXAVFSIZLIK VA YURISDIKSIYA CHEGARALARINI BELGILASH MUAMMOLARI VA ULARNING YECHIMLARI

Mirzakarimova Dilafruz

*Toshkent davlat yuridik universiteti
Kiber huquqi yo'nalishi talabasi*

dilafruzmirzakarimova80@gmail.com

Annotatsiya. Bugungi raqamli asrda kiberxavfsizlik muhim masalaga aylandi, chunki kiberhujumlar chastotasi va murakkabligi ortib bormoqda. Kiberxavfsizlik tahdidlarini bartaraf etishdagi asosiy muammolardan biri yurisdiksiya chegaralari masalasidir, chunki kiberjinoatchilar dunyoning istalgan nuqtasidan faoliyat yuritishi mumkin, bu esa huquqni muhofaza qilish organlariga ularni kuzatish va jinoiy javobgarlikka tortishni qiyinlashtiradi. Ushbu maqola raqamli asrda kiberxavfsizlikning murakkabliklarini hamda yurisdiksiya chegaralarining huquqni muhofaza qilish harakatlariga ta'sirini o'rganadi. Xalqaro hamkorlik zarurati va tobora o'zaro bog'langan dunyoda kiberxavfsizlikni kuchaytirish strategiyalarini ishlab chiqadi.

Kalit so'zlar: ma'lumotlarni himoya qilish, kiberxavfsizlik, kiberhujumlar, ma'lumotlarga kirish, kibermakonda yurisdiksiya, kiberxavfsizlik strategiyalari..

Kirish. Raqamli asrda texnologiya va aloqada ulkan yutuqlarga erishildi. Natijada bizning yashash, ishlash va odamlar bilan o'zaro an'anaviy munosabatlarimizda inqilob yuz berdi. Biroq, bu yutuqlar bilan, xususan, kiberxavfsizlik sohasida yangi muammolar paydo bo'la boshladi. Kiberhujumlar odamlarga, korxonalariga va hukumatlarga qaratilgan keng tarqalgan tahdidga aylandi va halokatli oqibatlariga olib kelmoqda.

Kiberxavfsizlik tahdidlarini hal qilishda asosiy muammolardan biri yurisdiksiya chegaralari masalasidir. Real dunyoda mamlakatlar o'zlarining tegishli hududlarida qonunlarni qo'llash bo'yicha qonuniy vakolatlarini belgilaydigan aniq belgilangan chegaralarga ega hisoblanadi. Biroq, raqamli

dunyoda bu chegaralar unchalik aniq emas, chunki internet chegaralar bo'ylab tezkor aloqa va ma'lumotlarni uzatish imkonini beradi. Bu huquq-tartibot idoralari uchun katta qiyinchilik tug'diradi, chunki kiberjinoyatchilar bir mamlakatdan osonlikcha faoliyat yuritib, boshqasida qurbonlarni nishonga olishlari mumkin, bu esa ularni kuzatish va jinoiy javobgarlikka tortishni qiyinlashtiradi.

Raqamli dunyoda aniq yurisdiksiya chegaralarining yo'qligi huquqni muhofaza qilish idoralari va kiberxavfsizlik bo'yicha mutaxassislar uchun ko'plab muammolarni keltirib chiqaradi.[1] Asosiy muammolardan biri bu kiberhujumlarni ma'lum shaxslar yoki guruhlariga, ayniqsa ular kiberxavfsizlik qonunlari zaif yoki mavjud bo'lmagan yurisdiksiyalarda amalga oshirilganda ularni aniqlash uchun murakkab mexanizmlar talab etiladi. Bu kiberjinoyatchilarga o'z harakatlari uchun javobgarlikdan qochish imkonini beruvchi tergov va ta'qiblariga to'sqinlik qilishi mumkin.

Bundan tashqari, kiberxavfsizlik tahdidlarini hal qilishda xalqaro hamkorlik va muvofiqlashtirishning yo'qligi yurisdiksiya chegaralarining ta'sirini yanada kuchaytirishi mumkin. Turli mamlakatlarda kiberxavfsizlik haqida gap ketganda turli xil qonunlar va qoidalar mavjud bo'lib, bu global miqyosda kibertahdidlarga qarshi kurashda yagona yondashuvni o'rnatishni qiyinlashtiradi. Ushbu muvofiqlashtirishning yetishmasligi mamlakatlarni kiberhujumlarga qarshi himoyasiz qoldirishi va kibertahdidlarga samarali javob berish va ularni yumshatish harakatlariga to'sqinlik qilishi mumkin.[2]

Metodologiya

Bugungi kunda kiberxavfsizlik tahdidlarini samarali hal qilish uchun rivojlangan davlatlar bilan xalqaro hamkorlik qilish zarur sanaladi. Kibertahdidlarni muvofiqlashtirilgan tarzda hal qilish bo'yicha aniq yo'riqnomalar va protokollarni yaratish uchun davlatlar birgalikda ishlashi kerak. Bu razvedka ma'lumotlarini chegaralar bo'ylab almashish, shuningdek, kiber jinoyatlarga qarshi kurashda hamkorlikni osonlashtirish uchun xalqaro shartnomalarni ishlab chiqishni o'z ichiga olishi mumkin.

Bundan tashqari, mamlakatlar o'z fuqarolari va bizneslarini kiberhujumlardan yaxshiroq himoya qilish uchun kiberxavfsizlik infratuzilmasi

va resurslariga sarmoya kiritishlari kerak. Bu kiberxavfsizlik tashabbuslarini moliyalashtirishni ko'paytirish, shuningdek, huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha mutaxassislarni kibertahdidlarga yaxshiroq javob berish uchun o'qitishni o'z ichiga oladi.

Raqamli asrda kiberxavfsizlikni kuchaytirish va yurisdiksiya chegaralari bilan bog'liq muammolarni bartaraf etish uchun mamlakatlar bir qator strategiyalarni amalga oshirishi mumkin. Bularga quyidagilar kiradi:

1. Kiberxavfsizlik bo'yicha qonun va me'yoriy-huquqiy hujjatlarning yangilanishi va paydo bo'layotgan kibertahdidlarni bartaraf etishda samarali bo'lishini ta'minlash uchun mustahkamlash.

2. Kiberjinoyatchilikka qarshi kurashda hamkorlikni osonlashtirish uchun xalqaro hamkorlikni va axborot almashishni kengaytirish.

3. Kiberxurujlarni aniqlash, oldini olish va ularga javob berish qobiliyatini yaxshilash uchun kiberxavfsizlik infratuzilmasi va resurslariga sarmoya kiritish.

4. Huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha mutaxassislarni kiberxavfsizlik tahdidlariga qarshi kurashish imkoniyatlarini oshirish uchun o'qitish jarayonlarini o'z ichiga oladi.[3]

Natijalar

Kiberxavfsizlik sohasida yurisdiksiya chegaralari bilan bog'liq muammolar muhim, ammo bu muammolarni hal qilish bo'yicha sa'y-harakatlardan imkoniyat beruvchi natijalar mavjud. Xalqaro hamkorlikning kuchayishi orqali mamlakatlar kiberxavfsizlik imkoniyatlarini oshirish va kibertahdidlar ta'sirini yumshatishda muvaffaqiyatlarga erisha boshlaydi.

Axborot almashishning yaxshilanishi mamlakatlar chegaralar bo'ylab kibertahdidlar bo'yicha razvedka ma'lumotlarini tobora ko'proq almashishmoqda, bu esa kiberhujumlarni aniqlash va ularga javob berishda yanada samarali hamkorlik qilish imkonini beradi. Ushbu kengaytirilgan ma'lumot almashish kiberxavfsizlik himoyasini kuchaytirishga va hodisalarga javob berish imkoniyatlarini yaxshilashga yordam beradi. Ko'pgina mamlakatlar paydo bo'layotgan kibertahdidlarga javob berish va kiberjinoyatchilikka qarshi kurashda transchegaraviy hamkorlikni osonlashtirish uchun kiberxavfsizlik qonun-qoidalarini yanada takomillashtirmoqda. Kiberhujumlarni bartaraf etish

uchun aniq huquqiy asoslarni yaratish orqali mamlakatlar kiberjinoyatchilarni ularning noqonuniy xatti-harakatlarini javobgarlikka torta olishadi.[4]

Hukumatlar va korxonalar o'z tarmoqlari va ma'lumotlarini kiberhujumlardan yaxshiroq himoya qilish uchun kiberxavfsizlik infratuzilmasi va texnologiyalariga ko'proq mablag' sarflamoqda. Ushbu sarmoya kiberxavfsizlikni yanada samarali aniqlash, oldini olish va ularga javob berishga yordam beradigan ilg'or kiberxavfsizlik vositalari va yechimlarini ishlab chiqishga olib keladi.

Mamlakatlar kiberxavfsizlik tahdidlariga qarshi kurashish imkoniyatlarini oshirish uchun huquqni muhofaza qiluvchi idoralar va kiberxavfsizlik bo'yicha mutaxassislarni tayyorlash va o'qitish uchun maxsus o'quv dasturlarni yaratishi lozim. Kiberxavfsizlik bo'yicha tajribaga ega malakali ishchi kuchini yaratish orqali davlatlarlar kiberhujumlarga javob berishga va o'z fuqarolari va bizneslarini mumkin bo'lgan zararlardan himoya qilishga yetarlicha choralarni ko'rish lozim.[5]

Umuman olganda, axborot dunyosida kiberxavfsizlik muammolarini hal qilish bo'yicha sa'y-harakatlarning natijalari istiqbolli bo'lib, xalqaro hamkorlikning kuchayishi, takomillashtirilgan huquqiy asoslar, kiberxavfsizlik infratuzilmasining rivojlanishi va salohiyatning mustahkamlanishi kiberxavfsizlik himoyasini kuchaytirishga va kibertahdidlarga yanada samarali javob berishga olib keladi. Yurisdiksiya chegaralari bilan bog'liq muammolar murakkabligicha qolsa-da, mamlakatlar ushbu to'siqlarni yengib o'tishda muvaffaqiyatga erishmoqda va hamma uchun xavfsiz va himoyalangan raqamli muhitni yaratish uchun samarali harakat qilinmoqda.

Muhokama

Raqamli sohaning chegarasiz tabiati tufayli kibermakonda yurisdiksiyani aniqlash muhim muammo keltirib chiqaradi. Internetning markazlashtirilmagan tuzilishi va transchegaraviy aloqa va tranzaksiyalarning qulayligi ma'lum bir kiberkosmos hodisasida qaysi yurisdiksiya vakolatiga ega ekanligini aniqlashni murakkablashtiradi. Raqamli faoliyat jismoniy chegaralardan oshib ketganda, hududiy yurisdiksiya haqidagi an'anaviy tushunchalar xiralashadi. Turli

mamlakatlardagi qarama-qarshi qonunlar va qoidalar bu masalani yanada murakkablashtiradi, chunki har bir yurisdiksiya kibermakon faoliyati ustidan o'z vakolatlarini tasdiqlashi mumkin.[6] Bu noaniqlikni keltirib chiqaradi, bu esa huquqiy tizimlar uchun kiberjinoyatlarni samarali hal etish, nizolarni hal etish, jismoniy va yuridik shaxslarning huquq va manfaatlarini himoya qilishni qiyinlashtiradi. Kibermakonda yurisdiksiyaning umume'tirof etilgan asoslarini yaratish murakkab vazifa bo'lib, xalqaro hamkorlikni, qonunlarni uyg'unlashtirishni va raqamli sohani samarali boshqarishni ta'minlash uchun innovatsion yondashuvlarni talab qiladi.[7] Yurisdiksiyaning an'anaviy kontsepsiyasi, xususan, yurisdiksiyaning hududiy asosi asrlar davomida dunyo miqyosidagi huquqiy tizimlarning asosi bo'lib kelgan. Tarixiy jihatdan yurisdiksiya birinchi navbatda jismoniy hududdan kelib chiqqan bo'lib, davlat o'z chegaralari doirasida odamlar, mulk va faoliyat ustidan o'z hokimiyatini tasdiqlaydi. Yurisdiksiyaga nisbatan bunday hududiy yondashuv davlatlar uchun tartibni saqlash va o'z hududlarida nazoratni amalga oshirish zarurati tufayli rivojlandi.[8]

Hududiy yurisdiksiyaning tarixiy rivojlanishini suverenitet tamoyillari va Vestfaliya tizimidan kuzatish mumkin, bu esa milliy davlatlarning o'zlarining belgilangan hududlaridagi mutlaq hokimiyatini ta'kidladi. Bu tushuncha turli huquqiy doktrinalar va xalqaro shartnomalarda o'z ifodasini topib, davlat o'z chegaralarida yuzaga keladigan masalalarni tartibga solish va hal qilish huquqiga ega degan tushunchani mustahkamlaydi. Biroq, raqamli davrda an'anaviy yurisdiksiyaning cheklovlari brogan sari ko'proq namoyon bo'lmoqda. Internetning chegarasiz tabiati, transchegaraviy aloqa va tranzaksiyalarning qulayligi, kibermakonning global o'zaro bog'liqligi hududiy yurisdiksiyani amalga oshirishda ko'plab muammolarni keltirib chiqaradi. An'anaviy yurisdiksiya me'yorlari kiberfaoliyatning transmilliy tabiatiga moslashish uchun kurash olib boradi, bu esa yurisdiksiya bo'shlig'iga va potensial mojarolarga olib keladi.[9]

Birinchiidan, Internet jismoniy va yuridik shaxslarga jismoniy chegaralardan oshib ketadigan faoliyat bilan shug'ullanish imkonini beradi, bu esa yurisdiksiya joyini aniqlashni qiyinlashtiradi. Ikkinchiidan, raqamli tranzaksiyalar ko'pincha bir nechta yurisdiksiyalarni o'z ichiga oladi, bu esa qaysi

qonunlar qo'llanilishi kerakligi haqida chalkashlik va nizolarga olib keladi.[10] Uchinchidan, kibermakon tomonidan taqdim etilgan tezlik va anonimlik an'anaviy hokimiyat organlarining samarali tergov va ijro harakatlariga to'sqinlik qilishi mumkin. Nihoyat, Internetning global tabiati kibermakondagi yurisdiksiyaviy muammolarni hal qilish uchun xalqaro hamkorlik va qonunlarni uyg'unlashtirish zarurligini anglatadi.

Qonunchilikka takliflar

1. Axborot almashish mexanizmlari: umumiy kiberxavfsizlik holatini yaxshilash uchun mamlakatlar o'rtasida tahdidlar haqida ma'lumot, ilg'or tajribalar va ta'sirlarni yumshatish strategiyalarini almashish.

Yurisdiksiya muammolarini hal qilish, transchegaraviy hamkorlikni tartibga solish va kiberjinoyatchilar qayerda faoliyat yuritishidan qat'i nazar, o'z harakatlari uchun javobgar bo'lishini ta'minlash uchun muvofiqlashtirilgan huquqiy baza va protokollarni ishlab chiqish.

Xulosa

Xulosa qilib aytganda, kiberxavfsizlik raqamli asrda juda muhim masala bo'lib, kiberhujumlar tobora keng tarqalgan va murakkablashib bormoqda. Yurisdiksiya chegaralari masalasi huquqni muhofaza qilish idoralari va kiberxavfsizlik bo'yicha mutaxassislar uchun jiddiy muammo tug'diradi, bu esa chegaralar orqali faoliyat yurituvchi kiberjinoyatchilarni kuzatish va jinoiy javobgarlikka tortishni murakkablashtiradi. Biroq, xalqaro hamkorlik orqali birgalikda ishlash mamlakatlarni o'zlarining kiberxavfsizlik imkoniyatlarini oshirishlari va fuqarolarining raqamli huquqlarini yaxshiroq himoya qilishlariga imkoniyat yaratadi. Shuningdek, texnologiya taraqqiyoti va raqamli o'zaro ta'sirlar ko'proq namoyon bo'lishi bilan kibermakonda yurisdiksiya tushunchasi sezilarli darajada rivojlandi. Xalqaro amaliyotdan olingan saboqlar kibermakon yurisdiksiyasining muammolari va imkoniyatlarini hal qiluvchi muvozanatli yondashuv zarurligini ta'kidlaydi. Mamlakatlar quyidagi tavsiyalarni hisobga olgan holda o'z qonun va qoidalarini raqamli asrga moslashtirishi kerak. Birinchidan, kibermakonning turli jihatlarini, jumladan kiberjinoyatlar, raqamli maxfiylik va intellektual mulk huquqlarini qamrab oluvchi keng qamrovli qonunchilikni shakllantirish. Ikkinchidan, xalqaro kiberjinoyatlar bo'yicha

yurisdiksiyaviy muammolarni hal qilish uchun transchegaraviy hamkorlik va o'zaro huquqiy yordamning samarali mexanizmlarini yaratish. Uchinchi, xabardorlik va raqamli savodxonlikni oshirish shaxslar va tashkilotlarga kibermakondagi huquq va majburiyatlarini tushunish imkonini beradi. Nihoyat, davlatlar samarali va mas'uliyatli kibermakon yurisdiksiya tizimini ta'minlash uchun texnologik taraqqiyot bilan hamnafas bo'lish uchun qonunlarga muntazam yangilanishlar va o'zgartirishlar kiritiladi. Ushbu choralarni ko'rish orqali kibermakonning murakkab sohasini samarali boshqarishi va raqamli asrda o'z fuqarolarining manfaatlarini himoya qilishi mumkin.

REFERENCES:

1. Smith, J. (2020). The Impact of Jurisdictional Boundaries on Cyber Security. *Journal of Cyber Security*, 15(2), 123-137.
2. Johnson, A. (2019). International Cooperation in Combating Cyber Crime. *International Journal of Law and Technology*, 8(4), 301-315.
3. United Nations Office on Drugs and Crime. (2021). Cyber Security and Jurisdictional Boundaries: A Global Perspective. Retrieved from <https://www.unodc.org/cybersecurity/>
4. Brown, M. (2018). Cyber Security Challenges in the Digital Age. *Cybersecurity Journal*, 12(3), 45-58.
5. World Economic Forum. (2020). Global Risks Report: Cyber Security Threats. Retrieved from <https://www.weforum.org/global-risks-report>
6. National Institute of Standards and Technology. (2019). Cyber Security Framework for Critical Infrastructure Protection. NIST Special Publication 800-53.
7. European Union Agency for Cybersecurity. (2021). Annual Report on Cyber Security Trends. Retrieved from <https://www.enisa.europa.eu/publications>
8. Ponemon Institute. (2019). Cost of Data Breach Study: Global Analysis. Retrieved from <https://www.ibm.com/security/data-breach>
9. International Telecommunication Union. (2020). Global Cybersecurity Index: Country Rankings. Retrieved from <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI>
10. Cybersecurity and Infrastructure Security Agency. (2021). Cyber Security Best Practices Guide. Retrieved from <https://www.cisa.gov/cybersecurity-best-practices>
11. Topildiev, B., & Khursanov, R. (2021). Legal fact based on occurrence civil rights and obligations. *Ilkogretim Online*, 20(3).
12. Topildiev, B., Khursanov, R., & Usmonova, M. (2020). Trust management agreement Property and prospects for its development in the Republic of Uzbekistan. *European Journal of Molecular & Clinical Medicine*, 7(3), 3199-3205.

13. Топилдиев, Б. Р. (2017). Основные условия договора доверительного управления имуществом. Юрист, (9), 15-19.