SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

KIBERJINOYATLAR BO‘YICHA XALQARO KONVENSIYALAR VA O‘ZBEKISTON QONUNCHILIGIDAGI MUVOFIQLIK

Tilovboyev Bunyodbek
O‘zbekiston Respublikasi Ichki ishlar vazirligi akademiyasi kursanti

https://doi.org/10.5281/zenodo.23494712

Annotatsiya: Ushbu ilmiy maqolada axborot-kommunikatsiya texnologiyalari rivojlanishi sharoitida kiberxavfsizlikni ta’minlash, kiberjinoyatchilikka qarshi kurashishning xalqaro-huquqiy mexanizmlari hamda ularning O‘zbekiston Respublikasi milliy qonunchiligidagi ifodasi tahlil qilingan. Xususan, Budapesht konvensiyasi qoidalari va BMT doirasidagi global tashabbuslarning milliy huquq tizimiga implementatsiyasi, shuningdek, milliy jinoiy va ma’muriy qonunchilikdagi muvofiqlik holati qiyosiy-huquqiy jihatdan o‘rganilgan.

Kalit so‘zlar: kiberjinoyat, axborot xavfsizligi, Budapesht konvensiyasi, raqamli dalillar, Jinoyat kodeksi, xalqaro hamkorlik, transchegaraviy jinoyatchilik, yurisdiksiya.

Zamonaviy raqamli transformatsiya, sun’iy intellekt, bulutli texnologiyalar va elektron to‘lov tizimlarining jadallashuvi insoniyat hayotini yengillashtirish bilan bir qatorda kiberjinoyatchilikning yangi va transchegaraviy shakllarini yuzaga keltirdi. An’anaviy jinoyatlardan farqli ravishda kiberjinoyatlar davlat chegaralari, geografik masofa va vaqt bilan cheklanmaydi [1].

Bunday qilmishlarning oldini olish, ularni tergov qilish va aybdorlarni javobgarlikka tortish har bir davlatdan alohida ichki choralar ko‘rish bilan birga xalqaro miqyosdagi normativ-huquqiy va institutsional uyg‘unlikni (muvofiqlikni) talab etadi. O‘zbekiston Respublikasida so‘nggi yillarda raqamli iqtisodiyot va kiberxavfsizlik sohasida mustahkam huquqiy asoslar yaratilayotgan bo‘lsa-da,

milliy qonunchilik normalarini kiberjinoyatchilikka qarshi kurash bo‘yicha xalqaro konvensiyalar standartlariga to‘liq moslashtirish dolzarb vazifa bo‘lib qolmoqda [2].

Kiberjinoyatlarga qarshi xalqaro maydonda eng asosiy va universal hujjat sifatida Yevropa Kengashining 2001-yil 23-noyabrda qabul qilingan «Kiberjinoyatchilik to‘g‘risida»gi Konvensiyasi (**Budapesht konvensiyasi**, ETS No. 185) e’tirof etiladi [3]. Mazkur konvensiya nafaqat Yevropa davlatlari, balki dunyoning 70 ga yaqin mamlakati (jumladan, AQSH, Yaponiya, Kanada kabi davlatlar) tomonidan ratifikatsiya qilingan.

Budapesht konvensiyasi asosan uchta o‘q ustiga qurilgan:

1. **Moddiy-huquqiy normalarni unifikatsiyalash:** Kompyuter ma’lumotlari va tizimlarining daxlsizligiga qarshi jinoyatlar (noqonuniy kirish, ushlab qolish, ma’lumotlarni o‘chirish yoki buzish), kompyuter vositasida sodir etiladigan qilmishlar (firibgarlik, soxtalashtirish), mualliflik huquqini buzish hamda bolalar pornografiyasiga qarshi qat’iy jazoiy normalarni belgilash;
2. **Protsessual-huquqiy mexanizmlar:** Elektron (raqamli) dalillarni tezkor saqlash, yozib olish, qidirish va olib qo‘yish bo‘yicha vakolatli organlarga aniq huquqiy richaglarni taqdim etish;
3. **Xalqaro hamkorlik va tezkor aloqa:** Transchegaraviy kiberhujumlarni tergov qilishda ma’lumot almashish uchun «24/7 aloqa tarmog‘i»ni (Network 24/7) yaratish [4].

Shu bilan birga, so‘nggi yillarda Birlashgan Millatlar Tashkiloti doirasida global kiberjinoyatchilikka qarshi yangi konvensiya loyihasini ishlab chiqish bo‘yicha Maxsus qo‘mitaning keng qamrovli faoliyati olib borilmoqda. Mazkur jarayonda barcha suveren davlatlarning manfaatlari va teng huquqli kiberhimoya kafolatlari ilgari surilmoqda [5].

O‘zbekiston Respublikasi kiberjinoyatchilikka qarshi ichki huquqiy bazani bosqichma-bosqich shakllantirib kelmoqda. Xususan:

- O‘zbekiston Respublikasi Jinoyat kodeksining XX¹ bobi bevosita **«Axborot texnologiyalari sohasidagi jinoyatlar»** deb nomlanib, 278¹–278⁷-moddalarida kompyuter axborotiga qonunga xilof ravishda kirish, zararli dasturlarni yaratish, axborotni yo‘q qilish yoki modifikatsiyalash kabi qilmishlar uchun jinoiy javobgarlik belgilangan [6].
- 2022-yilda qabul qilingan «Kiberxavfsizlik to‘g‘risida»gi Qonun milliy kiberfazoda axborot xavfsizligini ta’minlash, muhim axborot infratuzilmasi obyektlarini himoya qilish va ushbu yo‘nalishdagi davlat organlarining vakolatlarini huquqiy jihatdan mustahkamladi [7].

Biroq milliy qonunchiligimizdagi normalar xalqaro konvensiyalar talablari bilan qiyoslanganda, elektron dalillarni protsessual rasmiylashtirish, xalqaro huquqiy yordam ko‘rsatish tezkorligi va ayrim zamonaviy kiberhujum shakllarini (masalan, fishing, kriptoaktivlar vositasidagi kiberfiribgarlik) kvalifikatsiya qilish borasida muayyan tafovutlar va bo‘shliqlar mavjudligini ko‘rish mumkin.

O‘zbekiston Respublikasida kiberjinoyatlarni aniqlash, tergov qilish va fosh etish bo‘yicha ichki ishlar organlari hamda boshqa huquqni muhofaza qiluvchi idoralar amaliyotini o‘rganish shuni ko‘rsatadiki, sohadagi texnik va moddiy ta’minot rivojlanib borayotganiga qaramasdan, xalqaro konvensiyalar standartlari bilan amaliy qonunchilik o‘rtasida qator tizimli nomutanosibliklar saqlanib qolmoqda [8]. Xalqaro hujjatlar (xususan, Budapesht konvensiyasi va BMT loyihalari) talablari bilan milliy qonunchilikni qiyosiy tahlil qilish natijasida quyidagi asosiy tafovutlar va to‘siqlarni ajratib ko‘rsatish mumkin:

1. Moddiy-huquqiy normalar doirasidagi tafovutlar

O‘zbekiston Respublikasi Jinoyat kodeksining XX¹ bobi kiberjinoyatlarning ma’lum bir guruhini qamrab olgan bo‘lsa-da, kiberjinoyatchilikning yangi va murakkab usullarini to‘g‘ri kvalifikatsiya qilishda qonunchilikda bo‘shliqlar mavjud:

- **DDoS-hujumlar va servisni to‘xtatib qo‘yish:** Xalqaro tajribada axborot tizimlarining ishlashiga qasddan to‘sqinlik qilish (System interference) mustaqil jinoyat tarkibi hisoblanadi. Milliy Jinoyat kodeksining 278²-moddasida ushbu harakatlar asosan axborotni to‘sib qo‘yish bilan bog‘lanadi, biroq serverlarni sun’iy so‘rovlar bilan ortiqcha yuklash orqali butun xizmat faoliyatini falaj qilish holatlarini qamrab olishda amaliyotda qiyinchiliklar tug‘iladi [9].
- **Kiberfiribgarlik va kiberqurollar muomalasi:** Bugungi kunda bank kartalari ma’lumotlarini noqonuniy qo‘lga kiritish (fishing, vishing), kriptovalyutalar orqali mablag‘larni yuvish va "Darknet" tarmoqlarida kiberhujum vositalarini sotish alohida ixtisoslashgan norma sifatida emas, balki an’anaviy firibgarlik (JK 168-moddasi) yoki axborot sohasidagi umumiy normalar orqali baholanmoqda. Bu esa qilmishning o‘ziga xos ijtimoiy xavflilik darajasini to‘liq ochib bermaydi.

2. Elektron (raqamli) dalillarni to‘plash va mustahkamlashdagi protsessual muammolar

Budapesht konvensiyasining eng kuchli jihati — bu raqamli dalillarni saqlash va olib qo‘yishning qat’iy, ammo tezkor protsessual mexanizmini yaratganligidir. O‘zbekiston Jinoyat-protsessual kodeksida (JPK) esa quyidagi kamchiliklar ko‘zga tashlanadi:

- **Raqamli ma’lumotlarni tezkor saqlash (Expedited preservation) institutining yo‘qligi:** Internet-provayderlar va aloqa operatorlari bazalaridagi server loglari, IP-manzillar va marshrutizatsiya ma’lumotlari juda tez o‘chib ketadi (dinamik xarakterga ega). Amaldagi qonunchilik bo‘yicha tergovchining so‘rovi yoki sud ajrimini olish uchun ketadigan vaqt ichida serverdagi ma’lumotlar yo‘q qilinishi yoki o‘zgartirilishi xavfi yuqori [10].

- **Elektron dalillarning daxlsizligi (Chain of custody):** Raqamli vositalarni (serverlar, qattiq disklar, mobil qurilmalar) voqea joyidan olib qo‘yishda xesh-summalarni hisoblash, ma’lumotlarning butunligini texnik jihatdan kafolatlash bo‘yicha JPKda yagona va standartlashtirilgan qat’iy talablar to‘liq ifodalanmagan.

3. Xalqaro tezkor hamkorlik va yurisdiksiya muammosi

Kiberjinoyatchilar ko‘pincha O‘zbekiston hududidagi fuqarolarga nisbatan xorijiy davlatlarda joylashgan proksi-serverlar, VPN xizmatlari va xorijiy to‘lov tizimlari orqali zarba berishadi.

- Amaldagi xalqaro huquqiy yordam ko‘rsatish tizimi (diplomatik kanallar, Bosh prokuratura orqali yuboriladigan an’anaviy so‘rovlar) oylar davomida ko‘rib chiqiladi. Kiberfazoda esa bir necha soat ichida dalillar butunlay o‘chirib yuboriladi [11].
- O‘zbekistonning Budapesht konvensiyasiga a’zo emasligi sababli, uning «24/7 aloqa tarmog‘i»ga bevosita integratsiyalashuvi cheklangan bo‘lib, bu transchegaraviy jinoyatchilarning tergovdan qochib qolishiga imkon bermoqda.

Mazkur tizimli muammolar O‘zbekiston qonunchiligini xalqaro konvensiyalar talablari bilan yanada chuqurroq uyg‘unlashtirishni taqozo etadi.

O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashish samaradorligini oshirish va xalqaro miqyosda tergov harakatlarining uzviyligini ta’minlash qonunchilikni modernizatsiya qilishni hamda universal xalqaro-huquqiy standartlarga integratsiyalashuvni talab etadi. Ushbu yo‘nalishdagi faoliyatni takomillashtirish maqsadida quyidagi ilmiy-amaliy taklif va tavsiyalar ilgari suriladi:

1. **Budapesht konvensiyasiga qo‘shilish masalasini bosqichma-bosqich ko‘rib chiqish.**

O‘zbekistonning Yevropa Kengashining «Kiberjinoyatchilik to‘g‘risida»gi Konvensiyasiga (Budapesht konvensiyasi) qo‘shilishi yoki BMT doirasida ishlab chiqilayotgan global kiberjinoyatchilik konvensiyasiga faol a’zo bo‘lishi milliy tergov organlariga jahonning yetakchi kiberxavfsizlik markazlari bilan real vaqt rejimida axborot almashish («24/7 tarmog‘i») imkoniyatini taqdim etadi [12].

2. **Jinoyat-protsessual kodeksiga «Raqamli (elektron) dalillar» institutini kiritish.**

   JPKga elektron dalillarni to‘plash, ko‘zdan kechirish, olib qo‘yish va ularning daxlsizligini ta’minlash (Chain of custody) tartibini belgilovchi maxsus bob kiritish zarur. Shuningdek, tergovchiga internet-provayderlar va server egalaridan trafigi va log-fayllarni sud qaroriga qadar 90 kungacha shoshilinch muzlatib qo‘yish (tezkor saqlash — Expedited preservation) vakolatini beruvchi qonuniy mexanizm yaratilishi lozim [13].

3. **Jinoyat kodeksidagi axborot texnologiyalari sohasidagi normalarni kengaytirish.**

   Jinoyat kodeksining XX[1] bobini zamonaviy tahdidlarga moslashtirish, jumladan:

   - Kiberfiribgarlik (fishing, ijtimoiy injiniring, skimmerlar orqali talon-toroj qilish) bo‘yicha alohida modda kiritish;
   - Servisni rad etish hujumlari (DDoS/DoS) orqali axborot tizimining faoliyatini falaj qilganlik uchun jinoiy javobgarlikni alohida dispozitsiyada mustahkamlash;
   - Kriptoaktivlar va noqonuniy virtual aktivlar aylanishi vositasida kiberjinoyat sodir etishni javobgarlikni og‘irlashtiruvchi belgi sifatida kiritish [14].

4. **Kiberforensika (raqamli kriminalistika) markazlarini xalqaro akkreditatsiyadan o‘tkazish.**

   Ichki ishlar vazirligi va Bosh prokuratura tizimidagi raqamli ekspertiza laboratoriyalarining texnik quvvatini ISO/IEC 27037 (Raqamli dalillarni aniqlash, to‘plash va saqlash) xalqaro standartlari darajasiga yetkazish lozim. Bu milliy ekspertlar xulosalarining xorijiy sudlarda tan olinishiga zamin yaratadi [15].

5. **Xususiy sektor va yirik xalqaro platformalar bilan huquqiy hamkorlik mexanizmini yo‘lga qo‘yish.**

   Xalqaro messenjerlar, ijtimoiy tarmoqlar (Telegram, Meta, Google va boshqalar) hamda to‘lov tizimlari bilan tezkor huquqiy so‘rovlar almashinuvini ta’minlovchi idoralararo xalqaro protokollarni tuzish, ushbu platformalarning rasmiy vakolatxonalari bilan jinoyatlarni fosh etish bo‘yicha to‘g‘ridan-to‘g‘ri elektron aloqa kanalini shakllantirish kerak.

Xulosa qilib aytganda, kiberjinoyatchilikning transchegaraviy va dinamik tabiati milliy qonunchilikni alohida ajratilgan (lokal) tizim sifatida qo‘llash imkoniyatini cheklaydi. Jinoyatchilar zamonaviy axborot-kommunikatsiya vositalari, maxfiylashtirilgan kanallar va virtual aktivlar orqali chegaralarni osonlik bilan aylanib o‘tmoqda.

O‘zbekiston Respublikasining kiberxavfsizlikka oid milliy qonunchiligini ilg‘or xalqaro konvensiyalar standartlariga muvofiqlashtirish, elektron dalillar bilan ishlashning tezkor protsessual mexanizmlarini yaratish hamda global «24/7» tarmog‘i doirasida xalqaro operativ hamkorlikni kengaytirish milliy axborot makonining daxlsizligini va fuqarolarning raqamli huquqlarini ishonchli himoya qilishning eng asosiy kafolatidir.

REFERENCES:

1. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni. O‘RQ-764-son. 15.04.2022-y. // Qonunchilik ma’lumotlari milliy bazasi (lex.uz).
2. O‘zbekiston Respublikasi Prezidentining 2021-yil 29-noyabrdagi PF-27-son «O‘zbekiston Respublikasi jamoat xavfsizligi konsepsiyasini tasdiqlash to‘g‘risida»gi Farmoni // Qonunchilik ma’lumotlari milliy bazasi (lex.uz).
3. Council of Europe. Convention on Cybercrime (ETS No. 185). Budapest, 23.XI.2001. – Strasbourg: Council of Europe, 2001. – 28 p.
4. Clough J. Principles of Cybercrime. 2nd ed. – Cambridge: Cambridge University Press, 2015. – 464 p.
5. United Nations. Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. – New York: UN, 2024. – 45 p.
6. O‘zbekiston Respublikasining Jinoyat kodeksi. Rasmiy nashr. – Toshkent: Adolat, 2023. – 480 b.
7. O‘zbekiston Respublikasining «Axborotlashtirish to‘g‘risida»gi Qonuni. 560-II-son. 11.12.2003-y. // O‘zbekiston Respublikasi Oliy Majlisining Axborotnomasi. – 2004. – № 1-2. – 10-m.
8. Xayitovich, Y. D. (2026). TRANSPORT HUQUQI MUSTAQIL HUQUQ TARMOQI SIFATIDA: NAZARIY ASOSLAR, QIYOSIY TAHLIL VA O‘ZBEKISTON QONUNCHILIGINI TAKOMILLASHTIRISH MASALALARI. Eurasian Journal of Law, Finance and Applied Sciences, 6(2), 67-71.
9. Ziyodullayev M.Z., Matchanov A.A. va boshq. Huquqbuzarliklar profilaktikasi: Darslik. – Toshkent: O‘zbekiston Respublikasi IIV Akademiyasi, 2020. – 380 b.

10. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi. Rasmiy nashr. – Toshkent: Adolat, 2023. – 568 b.
11. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace. – Santa Barbara: Praeger, 2010. – 281 p.
12. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response. – Geneva: International Telecommunication Union (ITU), 2014. – 366 p.
13. Xayitovich, Y. J. (2021). Admission to the citizenship of the Republic of Uzbekistan in a simplified manner basics and conditions. ACADEMICIA: An International Multidisciplinary Research Journal, 11(3), 1421-1424.
14. Maras M.H. Cybercriminology. – Oxford: Oxford University Press, 2016. – 416 p.
15. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. – London: Academic Press, 2011. – 840 p.
16. linary Research Journal, 11(3), 1421-1424.