ZAMONAVIY HUQUQSHUNOSLIKNING AKTUAL MUAMMOLARI

XXIII-RESPUBLIKA ILMIY-AMALIY KONFERENSIYA

YAKUNLARI BO'YICHA ILMIY ISHLAR TO'PLAMI

Issue - 7(2026) Available at www.uznauka.uz

SUN’IY INTELLEKT SHAROITIDA KIBERDIPLOMATIYA: DAVLATLARNING KIBER MAKONDAGI MAS’ULIYATLI XATTI-HARAKATI NORMALARINI XALQARO-HUQUQIY TARTIBGA SOLISH

Sunnatillayev Sunnatilla Suhrob o‘g‘li

Mustaqil tadqiqotchi

E-mail: botirsamiyev803@gmail.com

Annotatsiya. *Maqolada kiberdiplomatiyaning raqamli diplomatiya tizimidagi o‘rni, uning predmeti va sub’ektlari tahlil qilinib, davlatlarning kiber makondagi mas’uliyatli xatti-harakati normalarining xalqaro-huquqiy shakllanish jarayoni tadqiq etilgan. Birlashgan Millatlar Tashkiloti doirasidagi hukumatlararo ekspertlar guruhi (GGE) va Ochiq turdagi ishchi guruh (OEWG) faoliyati natijasida shakllangan ixtiyoriy me’yorlar, ishonch choralari va salohiyatni oshirish mexanizmlari tizimlashtirilgan. Sun’iy intellekt texnologiyalarining tashqi siyosiy va harbiy-siyosiy faoliyatga tatbiq etilishi bilan bog‘liq yangi huquqiy muammolar — sintetik kontent va dezinformatsiya orqali ichki ishlarga aralashish, avtonom kiber vositalar uchun javobgarlik, attributsiya (nisbat berish) mezonlari — xalqaro huquq tamoyillari nuqtayi nazaridan baholangan. Yevropa Kengashining sun’iy intellekt bo‘yicha ramka konvensiyasi, Yevropa Ittifoqining sun’iy intellekt to‘g‘risidagi reglamenti va O‘zbekiston Respublikasining milliy*

siyosati qiyosiy tahlil qilinib, tartibga solishni takomillashtirish bo‘yicha takliflar ishlab chiqilgan.

Kalit so‘zlar: *kiberdiplomatiya, sun’iy intellekt, mas’uliyatli xatti-harakat normalari, GGE, OEWG, attributsiya, davlat javobgarligi, aralashmaslik tamoyili, dezinformatsiya, kiberxavfsizlik.*

Kiber makon zamonaviy davlatlararo munosabatlarning mustaqil maydoniga aylandi. Kritik infratuzilmaga qaratilgan hujumlar, saylov jarayonlariga axborot ta’siri va transchegaraviy ma’lumot oqimlari ustidan nazorat uchun kurash an’anaviy xavfsizlik masalalari bilan bir qatorda turadi. Bunday sharoitda davlatlarning kiber makondagi xatti-harakatini muvofiqlashtirishga qaratilgan maxsus yo‘nalish — kiberdiplomatiya shakllandi.[1]

Sun’iy intellekt texnologiyalari bu jarayonga yangi o‘lchov qo‘shdi. Generativ modellar yaratadigan sintetik matn, ovoz va videokontent axborot ta’siri operatsiyalari ko‘lamini kengaytirdi; avtomatlashtirilgan vositalar esa qaror qabul qilish tezligini inson aralashuvi imkoniyatidan ustun qildi. Bu xalqaro huquqning javobgarlik, aralashmaslik va suverenitet institutlarini yangicha talqin qilishni taqozo etmoqda.[2]

Mavzuning dolzarbligi shundaki, kiber makondagi xatti-harakat normalari asosan majburiy kuchga ega bo‘lmagan hujjatlar orqali shakllangan. 2013, 2015 va 2021-yillardagi hukumatlararo ekspertlar guruhi hisobotlari hamda Ochiq turdagi

[1] Diplo Foundation. Cyber diplomacy: concepts and practice. — URL: https://www.diplomacy.edu/

[2] UNIDIR. Framework for Responsible State Behaviour in Cyberspace. — URL: https://unidir.org/

ishchi guruh hujjatlari xalqaro huquqning kiber makonga qo‘llanilishini tasdiqlagan bo‘lsa-da, ular ixtiyoriy me’yorlar majmuidan iborat.[3]

Tadqiqotning maqsadi — kiberdiplomatiyaning huquqiy tabiatini aniqlash, mas’uliyatli xatti-harakat normalarining normativ maqomini baholash va sun’iy intellekt sharoitida ularni takomillashtirish yo‘nalishlarini asoslashdan iborat. Qiyosiy-huquqiy, formal-yuridik, tizimli tahlil va huquqiy prognozlashtirish metodlari qo‘llanilgan. Ilmiy yangiligi — sun’iy intellekt vositalari qo‘llanilgan kiber operatsiyalar uchun javobgarlikni belgilashda “nazorat darajasi” mezoniga asoslangan bosqichli yondashuvni taklif etishdan iborat.

Kiberdiplomatiya — davlatlarning kiber makondagi manfaatlarini himoya qilish va bu sohadagi xalqaro normalarni shakllantirishga qaratilgan diplomatik faoliyat turi. U raqamli diplomatiyaning tarkibiy qismi bo‘lsa-da, predmeti bilan farqlanadi: raqamli diplomatiya faoliyatning vositasi va shakliga oid bo‘lsa, kiberdiplomatiya muzokaralar predmetiga — kiberxavfsizlik, internet boshqaruvi va raqamli texnologiyalarning xalqaro rejimiga — qaratilgan.

Uning huquqiy tabiati ikki jihatdan namoyon bo‘ladi. Birinchidan, u norma yaratish jarayonining bir qismi sifatida davlat amaliyoti va opinio juris shakllanishiga hissa qo‘shadi. Ikkinchidan, u nizolarni tinch yo‘l bilan hal etish vositasi sifatida BMT Nizomining 33-moddasidagi muzokara instituti bilan bog‘lanadi. Shu ma’noda kiberdiplomatik faoliyat natijalari — qo‘shma

[3] Report of the Group of Governmental Experts. — UN Doc. A/68/98 (2013); A/70/174 (2015); A/76/135 (2021).

bayonotlar, milliy pozitsiya hujjatlari, ishonch choralari to‘g‘risidagi kelishuvlar — odat huquqi normalari shakllanishi uchun material bo‘lib xizmat qiladi.

BMT doirasidagi hukumatlararo ekspertlar guruhi 2013-yilgi hisobotida xalqaro huquq, xususan BMT Nizomi kiber makonga qo‘llanilishini birinchi marta rasman tasdiqladi. 2015-yilgi hisobotda ixtiyoriy me’yorlar to‘plami shakllantirildi: kritik infratuzilmaga hujum qilmaslik, boshqa davlatning CERT guruhlari faoliyatiga zarar yetkazmaslik, o‘z hududidan zararli faoliyatga yo‘l qo‘ymaslik, yetkazib berish zanjiri yaxlitligini ta’minlash.[4]

2021-yilgi hisobot me’yorlarni qo‘llash bo‘yicha qo‘shimcha tushuntirishlar berdi va milliy pozitsiyalarni e’lon qilish amaliyotini rag‘batlantirdi. Shunday bo‘lsa-da, xalqaro gumanitar huquqning kiber operatsiyalarga qo‘llanilishi va qarshi choralar rejimi bo‘yicha davlatlar o‘rtasida tafovutlar saqlanmoqda.

Xalqaro odat huquqining asosiy tamoyillaridan biri — davlatlarning ichki ishlariga aralashmaslik. Xalqaro Sud amaliyotiga ko‘ra aralashuv deb topilishi uchun harakat davlatning erkin qaror qabul qilish sohasiga qaratilgan bo‘lishi va majburlash (coercion) elementini o‘z ichiga olishi lozim.[5] Sun’iy intellekt yordamida yaratilgan sintetik materiallar orqali saylov jarayoniga ta’sir ko‘rsatish holatlarida aynan majburlash elementini isbotlash murakkab: bunday ta’sir ovoz berish erkinligini bevosita cheklamaydi, balki saylovchining axborot muhitini o‘zgartiradi.

[4] Report of the Group of Governmental Experts. — UN Doc. A/70/174 (2015). — 13-band.

[5] Nicaragua v. United States of America, Merits, Judgment // ICJ Reports. — 1986. — 205-band.

Doktrinada ikki yondashuv taklif etiladi: majburlash tushunchasini kengaytirib, unga axborot muhitini tizimli manipulyatsiya qilishni kiritish; yoki suverenitet tamoyilining mustaqil buzilishi konsepsiyasidan foydalanish. Ikkalasi ham davlat amaliyotida hali yetarli tasdiq topmagan.

Davlatlarning xalqaro huquqbuzarliklari uchun javobgarligi to‘g‘risidagi moddalar loyihasiga ko‘ra, davlatga uning organlari, shuningdek davlat topshirig‘i yoki nazorati ostida harakat qilgan shaxslar xatti-harakati nisbat beriladi.[6] Sun’iy intellektga asoslangan avtonom kiber vositalar qo‘llanilganda nazorat darajasini aniqlash murakkablashadi: tizim mustaqil ravishda nishonni tanlashi yoki oldindan belgilanmagan tarzda tarqalishi mumkin.

Bunday holatda javobgarlikni belgilashda bosqichli yondashuv maqsadga muvofiq: birinchi bosqichda tizimni ishga tushirish to‘g‘risidagi qaror davlat organi tomonidan qabul qilinganligi aniqlanadi; ikkinchi bosqichda oldindan ko‘ra bilish mumkin bo‘lgan oqibatlar doirasi baholanadi; uchinchi bosqichda ehtiyotkorlik burchi (due diligence) bajarilgan-bajarilmagani tekshiriladi. Bu yondashuv avtonomiya darajasi javobgarlikdan qochish uchun asos bo‘lib qolishining oldini oladi.

Kiber operatsiyani davlatga nisbat berish texnik, huquqiy va siyosiy jihatlarni qamrab oladi. Xalqaro huquqda attributsiya uchun zarur dalil standarti belgilanmagan, bu esa qarshi choralar asosliligini baholashda noaniqlik keltirib chiqaradi. Sun’iy intellekt vositalari hujum manbasini yashirish imkoniyatlarini

[6] Draft Articles on Responsibility of States for Internationally Wrongful Acts / International Law Commission. — 2001. — 4- va 8-moddalar.

kengaytirmoqda, shu bilan birga aniqlash imkoniyatlarini ham oshiradi.[7] Shu sababli attributsiya bo‘yicha umumiy protsessual standartlarni ishlab chiqish kiberdiplomatiyaning muhim vazifasi hisoblanadi.

2024-yilda Yevropa Kengashi doirasida sun’iy intellekt, inson huquqlari, demokratiya va huquq ustuvorligi to‘g‘risidagi ramka konvensiyasi imzolash uchun ochildi. Bu — sohadagi birinchi xalqaro shartnoma bo‘lib, unda sun’iy intellekt tizimlarining butun hayotiy sikli davomida inson huquqlarini himoya qilish majburiyati mustahkamlangan.[8] Konvensiya Yevropa Kengashi a’zosi bo‘lmagan davlatlar uchun ham ochiq, ya’ni u universal standart shakllanishiga asos bo‘lishi mumkin.

Yevropa Ittifoqining sun’iy intellekt to‘g‘risidagi reglamenti esa xavf darajasiga asoslangan model joriy etadi: taqiqlangan amaliyotlar, yuqori xavfli tizimlarga qo‘yiladigan talablar va shaffoflik majburiyatlari belgilanadi.[9] Ushbu model milliy qonunchilikni shakllantirishda keng qo‘llanilayotgan yondashuvga aylandi va uchinchi davlatlar qonunchiligiga ham ta’sir ko‘rsatmoqda.

O‘zbekistonda sun’iy intellekt va kiberxavfsizlik sohasidagi davlat siyosati “Raqamli O‘zbekiston — 2030” strategiyasi hamda sun’iy intellekt texnologiyalarini rivojlantirish bo‘yicha dasturiy hujjatlar doirasida amalga

[7] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / NATO CCDCOE. — Cambridge: Cambridge University Press, 2017. (Attributsiyaga oid qoidalar).

[8] Council of Europe Framework Convention on Artificial Intelligence. — CETS No. 225. — 2024.

[9] Regulation (EU) 2024/1689 (Artificial Intelligence Act) // OJ EU.

oshirilmoqda.[10] Kiberxavfsizlik to‘g‘risidagi qonunchilik bazasi shakllantirilib, kritik axborot infratuzilmasi ob’ektlarini himoya qilish va kiber hodisalarga javob berish tartibi belgilangan.

Shu bilan birga, bir qator vazifalar dolzarb qolmoqda. Birinchidan, xalqaro huquqni kiber makonga qo‘llash borasidagi rasmiy milliy pozitsiya e’lon qilinmagan; bunday hujjat davlat amaliyoti sifatida qayd etilardi. Ikkinchidan, Markaziy Osiyoda kiber hodisalar bo‘yicha axborot almashinuvining doimiy mexanizmi yo‘q. Uchinchidan, sun’iy intellektdan davlat boshqaruvida foydalanishga oid huquqiy kafolatlar to‘liq ishlab chiqilmagan.

1. Xalqaro huquqning kiber makonga qo‘llanilishi bo‘yicha rasmiy milliy pozitsiya hujjatini ishlab chiqish va e’lon qilish. Bu davlat amaliyotini shakllantirishga hissa qo‘shadi va xalqaro muzokaralarda izchillikni ta’minlaydi.

2. Attributsiya bo‘yicha protsessual standartlarni ilgari surish: dalillash mezonlari, ekspertizaning mustaqilligi va oshkoralik darajasini belgilovchi model qoidalarni BMT jarayonlarida taklif etish asossiz ayblovlar xavfini kamaytiradi.

3. Sun’iy intellekt qo‘llanilgan kiber operatsiyalar uchun javobgarlikning bosqichli mezonlarini mustahkamlash. Nazorat darajasi, oldindan ko‘ra bilish va ehtiyotkorlik burchiga asoslangan yondashuv avtonomiya orqali javobgarlikdan qochishning oldini oladi.

[10] O‘zbekiston Respublikasi Prezidentining 2020 yil 5 oktabrdagi PF-6079-son Farmoni. — URL: https://lex.uz/docs/-5031048

4. Mintaqaviy ishonch choralari mexanizmini yaratish: Markaziy Osiyo doirasida aloqa nuqtalari tarmog‘i, qo‘shma mashg‘ulotlar va kiber hodisalar bo‘yicha ogohlantirish tizimini institutsionalizatsiya qilish.

5. Sintetik kontent shaffofligi bo‘yicha xalqaro standartlarni qo‘llab-quvvatlash: sun’iy intellekt yaratgan materiallarni belgilash va manba tarixini kuzatish mexanizmlari dezinformatsiyaga qarshi samarali vosita bo‘lishi mumkin.

6. Diplomatik xizmat tizimida kiberdiplomatiya bo‘yicha mutaxassislar tayyorlash va xalqaro huquq hamda axborot texnologiyalari bilimlarini uyg‘unlashtirgan o‘quv dasturlarini joriy etish.

O‘tkazilgan tahlil shuni ko‘rsatadiki, kiberdiplomatiya bugungi kunda xalqaro huquq normalari shakllanishining muhim maydoniga aylangan. Davlatlarning kiber makondagi mas’uliyatli xatti-harakati me’yorlari mazmunan yetarlicha ishlab chiqilgan bo‘lsa-da, ularning huquqiy maqomi ixtiyoriy bo‘lib qolmoqda va ijro mexanizmlari bilan ta’minlanmagan. Sun’iy intellekt texnologiyalarining tarqalishi bu bo‘shliqni yanada sezilarli qilmoqda.

Eng real yo‘l — bosqichma-bosqich yondashuv: qisqa muddatda ishonch choralari va milliy pozitsiyalar orqali huquqiy aniqlikni oshirish; o‘rta muddatda attributsiya va javobgarlik bo‘yicha standartlarni shakllantirish; uzoq muddatda mavjud tamoyillarni aniqlashtiruvchi majburiy hujjat qabul qilish. O‘zbekiston uchun bu jarayonda faol ishtirok milliy kiberxavfsizlik tizimining huquqiy asoslarini mustahkamlaydi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Birlashgan Millatlar Tashkiloti Nizomi, 1945-yil 26-iyun.

2. Report of the Group of Governmental Experts, UN Doc. A/68/98, 2013.

3. Report of the Group of Governmental Experts, UN Doc. A/70/174, 2015.

4. Report of the Group of Governmental Experts, UN Doc. A/76/135, 2021.

5. Open-Ended Working Group (OEWG) hisobotlari, 2021—2025.

6. United Nations, Global Digital Compact, annexed to the Pact for the Future, 2024.

7. UN General Assembly resolution A/RES/78/265, 2024.

8. Draft Articles on Responsibility of States for Internationally Wrongful Acts, ILC, 2001.

9. Nicaragua v. United States of America, ICJ Reports, 1986.

10. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, NATO CCDCOE, 2017.

11. Council of Europe Framework Convention on Artificial Intelligence, CETS No. 225, 2024.

12. Regulation (EU) 2024/1689 (Artificial Intelligence Act).

13. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni.

14. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni.

15. UNIDIR, Responsible State Behaviour in Cyberspace, 2026.