



KIBERMAKONDA DAVLAT SUVERENITETI. NAZARIY VA HUQUQIY YONDASHUVLAR

Ma'murova Yorqinoy Qurvanali qizi

TDTrU yurisprudensiya (xalqaro transport huquqi)yo 'nalishi

e-mail: yorqinoymamurova63@gmail.com

Annotatsiya: Mazkur maqolada kibermakonda davlat suvereniteti tushunchasining nazariy va huquqiy asoslari tahlil etiladi. Klassik suverenitet konsepsiyasidan raqamli suverenitetga o'tish jarayoni, xalqaro huquq normalarining kibermakonga qo'llanilishi va cheklovlari ko'rib chiqiladi. Ushbu maqolaning dolzarbligi, milliy va jahon qonunchiligida kibermakonda suverenitetni ta'minlash masalalari va xalqaro standartlarni implementatsiya qilishdagi dolzarb muammolari muhokama qilinadi. Tadqiqot davomida jahon olimlarining fikrlari, foydali havolalar beriladi.

Kalit so'zlar: kibermakon, davlat suvereniteti, kibersuverenitet, xalqaro huquq, Tallinn Manual, raqamli hudud, aralashmaslik prinsipi

KIRISH

Zamonaviy raqamli transformatsiya sharoitida davlat boshqaruvi va ijtimoiy munosabatlarning kibermakonga ko'chishi kiberxavfsizlik tushunchasining mazmuni va huquqiy tabiatini yangicha nazariy tahlil qilishni taqozo etmoqda. Davlat suvereniteti an'anaviy ravishda muayyan hududiy chegaralar bilan bog'liq bo'lsa-da, kiber-makonning virtual va transchegaraviy tabiati ushbu tushunchani huquqiy talqin qilishda yangi yondashuvlarni, xususan, "raqamli chegaralar" daxlsizligini ta'minlashni talab qilmoqda. Kiberxavfsizlik bugungi kunda umumiy davlat xavfsizligining strategik tarkibiy qismi sifatida namoyon bo'lib, davlatning kiber-siyosat yurituvchi asosiy huquqiy subyekti sifatidagi mas'uliyatini oshirmoqda. Shu nuqtayi nazardan, xalqaro huquqning fundamental prinsiplari hisoblangan suverenitet va boshqa davlatlarning ichki ishlariga aralashmaslik



qoidalarini kibermakonga implementatsiya qilish hamda davlatlarning kibermakondagi huquqiy mas'uliyat chegaralarini aniqlashtirish dolzarb ilmiy va amaliy ahamiyatga ega. Mazkur maqolada kibermakonda davlat suverenitetining nazariy-huquqiy asoslari va uning davlat majburiyatlari bilan o'zaro nisbati tahlil qilinadi

Material va metodlar

Davlat suvereniteti xalqaro huquqning asosiy tamoyillaridan biri bo'lib, klassik talqinda davlatning o'z hududi, aholisi va ichki ishlariga to'la mustaqilligi sifatida qaraladi. Raqamli transformatsiya sharoitida kibermakon bu tushunchani yangi mazmun bilan boyitdi: suverenitet nafaqat fizik hudud, balki axborot infratuzilmasi, raqamli ma'lumotlar oqimi va kiberooperatsiyalar ustidan nazorat shaklida namoyon bo'ladi.[1]

Kibermakonda suverenitet masalasi birinchi marta keng ilmiy muhokamaga 2000-yillarning o'rtalarida chiqdi. 2007 yilda Estoniyaga nisbatan amalga oshirilgan keng ko'lamli kiberhujumlar bu masalani nazariy doiradan siyosiy amaliyot sohasiga olib chiqdi [2]. Mazkur hodisa shuni ko'rsatdiki, davlatning raqamli infratuzilmasiga qarshi yo'naltirilgan hujumlar uning suverenitetini amalda cheklab qo'yishi mumkin, ammo xalqaro huquqda bunday holatlarni tartibga soluvchi aniq normalar mavjud emasdi.

Nazariy jihatdan kibermakonda suverenitetga uchta asosiy yondashuv shakllangan. Birinchisi — **“hududiy yondashuv”** bo'lib, unga ko'ra davlat o'z hududida joylashgan barcha axborot-kommunikatsiya infratuzilmasi ustidan to'liq nazoratni amalga oshirishga haqlidir. Bu model, asosan, Xitoy va Rossiya Federatsiyasi tomonidan qo'llab-quvvatlanadi.[3] Ikkinchi yondashuv — **“funksional yondashuv”** bo'lib, xalqaro huquqning mavjud tamoyillari kibermakonga tatbiq etilishi mumkin, ammo qo'shimcha maxsus normalar ishlab chiqilishi zarur, degan g'oyaga asoslanadi. Bu pozitsiyani G'arb demokratiyalari, xususan, AQSh va Yevropa Ittifoqi davlatlari ushlab turadi Uchinchi yondashuv — **“cheksiz maydon” nazariyasi** bo'lib, kibermakoni hech qaysi davlat to'liq nazorat



qila olmaydigan global umumiy maydon deb hisoblaydi va bu sohadagi davlatlararo munosabatlarni yangi xalqaro shartnomalar orqali tartibga solishni taklif etadi[4]

Xalqaro huquq kibermakonga to'g'ridan-to'g'ri qo'llaniladi, chunki u real oqibatlar keltirib chiqaruvchi muhitdir. Eng muhim hujjatlardan biri – “Tallinn Manual 2.0” qoidalari hisoblanadi. Qo'llanmaning 4-qoidasiga ko'ra: “Davlat boshqa davlatning suverenitetini buzuvchi kiberoperatsiyalarni amalga oshirmasligi kerak” ekanligi belgilab qo'yilgan.[5]. Ushbu qoidalar “soft law” ko'rinishida bo'lib, xalqaro huquqiy nizolar vujudga kelganda qo'llanilishi mumkin.

O'zbekiston kibermakonda suverenitetni mustahkamlash bo'yicha izchil siyosat yuritmoqda. 2022-yilda “Kiberxavfsizlik to'g'risida” gi qonun qabul qilingan bo'lib, kiberxavfsizlik sohasida davlat tomonidan tartibga solinadigan asosiy normativ huquqiy hujjatlardan biri sanaladi. Qonunning 11-moddasiga ko'ra, O'zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organ ekanligi belgilab qo'yilgan.[6] “Raqamli O'zbekiston – 2030” strategiyasi (PF-6079, 2020) ma'lumotlar lokalizatsiyasi, milliy cloud platforma va kiber infratuzilmani rivojlantirishni belgilaydi. 2024–2025 yillarda qabul qilingan qo'shimcha o'zgartirishlar muhim infratuzilma ob'ektlarini himoya qilish mexanizmlarini yanada kuchaytirdi. Shu bilan birga, bu jarayon axborot erkinligi va xalqaro investorlar manfaatlari o'rtasidagi muvozanatni saqlash muammosini keltirib chiqarmoqda.

Kibermakonda davlat suvereniteti zamonaviy xalqaro huquqning eng dolzarb masalalaridan biridir. O'zbekiston uchun milliy qonunchilikni xalqaro standartlarga moslashtirish va suverenitetni himoya qilish mexanizmlarini takomillashtirish dolzarb vazifadir.

XULOSA. An'anaviy suverenitet tushunchasi kibermakoning o'ziga xos xususiyatlari chegara tanlamasligi, anonimlik, tezkor ta'sir ko'rsatish imkoniyati bilan to'liq mos kelmaydi. Vestfal suverenitet modeli asosida shakllangan xalqaro huquq normalari hududiy chegara va jismoniy nazorat tamoyillariga tayanadi, kibermakonda esa bu tamoyillarni qo'llash jiddiy metodologik va amaliy



qiyinchiliklarni keltirib chiqaradi. Shu sababli kibermakonda suverenitetni an'anaviy tushunchaning oddiy kengaytmasi sifatida emas, balki yangi nazariy-huquqiy kategoriya sifatida qarab chiqish zarurati tobora oydinlashmoqda.

Xalqaro huquqiy madaniyatning yetarli darajada shakllanmaganligi kibermakonda davlatlararo munosabatlarda huquqiy noaniqlikni keltirib chiqarmoqda. Tallinn 2.0 qo'llanmasi va boshqa xalqaro hujjatlar muhim qadam bo'lsa-da, ular majburiy huquqiy kuchga ega emas. Bu holat kibermakon uchun maxsus, majburiy kuchga ega bo'lgan xalqaro konvensiya yoki shartnoma ishlab chiqish zarurligini yanada dolzarb qilmoqda.

O'zbekiston milliy qonunchiligida kibermakonda suverenitetni ta'minlash mexanizmlari yetarli darajada shakllangan bo'lsa-da, bir qator muammolar saqlanib qolmoqda. Axborot erkinligi va milliy xavfsizlik o'rtasidagi muvozanat, xalqaro standartlarni to'liq implementatsiya qilishdagi qiyinchiliklar hamda davlat-xususiy sheriklikning yetarli rivojlanmaganligi shular jumlasidandir.

Aniqlangan muammolardan kelib qonunchilikka quyidagi takliflarni berish mumkin:

- “Kiberxavfsizlik to'g'risida”gi Qonunga kibermakonda suverenitet buzilishining aniq huquqiy mezonlarini kiritish
- Milliy “raqamli suverenitet” strategiyasini ishlab chiqish va uni xalqaro hujjatlar Tallinn Manual 2.0 va boshqa hujjatlar bilan uyg'unlashtirish hamda oliy ta'lim muassasalarida “Kiber huquq” sifatida o'qitish;

Kibermakonda davlat suvereniteti — bu bir martalik hal qilinishi mumkin bo'lgan muammo emas, balki texnologiyalar rivojlanishi bilan birga doimiy ravishda yangi qirralarni namoyon etuvchi dinamik huquqiy-siyosiy kategoriyadir. Ushbu sohadagi tadqiqotlarni davom ettirish, xalqaro hamkorlikni kuchaytirish va milliy huquqiy bazani takomillashtirish bugungi kunda barcha davlatlar oldida turgan eng dolzarb vazifalardan biri bo'lib qolmoqda.



REFERENCE

1. Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press
<https://www.cambridge.org/core/books/abs/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/sovereignty/6BA0C5B9829FD15D997B8C973C395E16>
2. Tikk, E., Kaska, K., Rünneri, K., Kert, M., Talihärm, A. M., & Vihul, L. (2008). *Cyber Attacks Against Georgia: Legal Lessons Identified*. NATO CCDCOE
<https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/>
3. Demchak, C. C., & Dombrowski, P. (2011). Rise of a cybered Westphalian age. *Strategic Studies Quarterly*, 5(1), 32–61.
<https://www.files.ethz.ch/isn/153779/spring11.pdf>
4. Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press
https://www.researchgate.net/publication/344506993_Networks_and_States_The_Global_Politics_of_Internet_Governance
5. Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations
[https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael N. Schmitt Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations-Cambridge University Press 2017 .pdf](https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press_2017_.pdf)
6. Kiberxavfsizlik to'g'risida- <https://lex.uz/uz/docs/-5960604#-5963345>