Kibermakonda due diligence prinsipining xalqaro-huquqiy ahamiyati

Mashrabjonova Asilaxon Anvarjon qizi
Jahon qtisodiyoti va diplomatiya universiteti
1-bosqich magistranti

Annotatsiya. Mazkur tezisda kibermakonda due diligence (zaruriy ehtiyotkorlik) prinsipining xalqaro-huquqiy mazmuni va ahamiyati tahlil qilingan. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi hamda transmilliy kiberxavflarning ortib borishi sharoitida davlatlarning kiberfazodagi huquq va majburiyatlarini aniqlash masalasi dolzarb ahamiyat kasb etmoqda. Tadqiqot davomida due diligence prinsipining xalqaro huquqdagi shakllanishi, uning xalqaro sud amaliyotidagi rivojlanishi hamda kibermakonga tatbiq etilishining nazariy va amaliy jihatlari o‘rganilgan.

Tadqiqot natijasida due diligence prinsipi davlatlarning kibermakondagi javobgarligini belgilovchi muhim xalqaro-huquqiy tamoyillardan biri ekanligi asoslab berilgan. Muallif tomonidan ushbu prinsipni O‘zbekiston Respublikasining milliy kiberxavfsizlik siyosati va qonunchiligiga bosqichma-bosqich implementatsiya qilish zarurligi ta’kidlangan.

Mazkur tadqiqot natijalari xalqaro kiberxavfsizlik sohasidagi ilmiy izlanishlarni rivojlantirish, milliy qonunchilikni takomillashtirish hamda xalqaro hamkorlik mexanizmlarini rivojlantirishda amaliy ahamiyatga ega.

Kalit so‘zlar: due diligence, kiberxavfsizlik, kiberfazo, xalqaro huquq, davlat javobgarligi, Tallinn Manual, kiberhujum, xalqaro hamkorlik, kiberxavfsizlik siyosati.

Аннотация. В данной статье анализируется международно-правовое содержание и значение принципа due diligence в киберпространстве. Развитие информационно-коммуникационных технологий и рост транснациональных киберугроз обуславливают необходимость определения прав и обязанностей государств в киберпространстве. В ходе исследования рассматриваются становление принципа due diligence в международном праве, его развитие в международной судебной практике, а также теоретические и практические аспекты его применения в киберпространстве.

По результатам исследования обосновано, что принцип due diligence является одним из важнейших международно-правовых принципов, определяющих ответственность государств в киберпространстве. Также отмечается необходимость имплементации данного принципа в национальную политику кибербезопасности Республики Узбекистан.

Ключевые слова: due diligence, кибербезопасность, киберпространство, международное право, ответственность государств, кибератака, Tallinn Manual, международное сотрудничество.

Abstract. This article analyzes the international legal nature and significance of the due diligence principle in cyberspace. The rapid development of information and communication technologies and the growing number of transnational cyber threats require the determination of states' rights and obligations in cyberspace. The study examines the development of the due diligence principle in international law, its evolution in international judicial practice, and the theoretical and practical aspects of its application in cyberspace.

The study concludes that the due diligence principle has become one of the most important international legal principles determining state responsibility in cyberspace. The necessity of implementing this principle into the national cybersecurity policy of the Republic of Uzbekistan is also emphasized.

Keywords: due diligence, cybersecurity, cyberspace, international law, state responsibility, cyberattack, Tallinn Manual, international cooperation.

Kirish. XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kibermakon xalqaro munosabatlarning muhim tarkibiy qismiga aylandi. Davlat boshqaruvi, moliyaviy tizimlar, energetika, transport, mudofaa va aloqa sohalarining raqamlashtirilishi kiberxavfsizlikni milliy va xalqaro xavfsizlikning muhim elementi sifatida shakllantirdi. Shu bilan birga, kiberjinoyatlar va davlatlararo kiberoperatsiyalar sonining ortib borishi xalqaro huquq oldiga yangi vazifalarni qo‘ymoqda.

Kiberhujumlarning o‘ziga xos xususiyati shundaki, ular davlat chegaralarini tan olmaydi va ko‘pincha bir necha davlat hududi orqali amalga oshiriladi. Natijada kiberhujumni amalga oshirgan shaxs yoki davlatni aniqlash, ularning xalqaro javobgarligini belgilash hamda zarar yetkazilgan davlat manfaatlarini himoya qilish murakkablashmoqda[1].

Bugungi kunda xalqaro huquqda eng ko‘p muhokama qilinayotgan masalalardan biri davlatlarning kibermakondagi majburiyatlari hisoblanadi. Davlat o‘z hududidan boshqa davlatlarga zarar yetkazuvchi kiberfaoliyat amalga oshirilishiga yo‘l qo‘ymasligi kerakmi? Agar bunday faoliyat nodavlat subyektlar tomonidan amalga oshirilgan bo‘lsa, davlat javobgar bo‘ladimi? Mazkur savollar xalqaro huquqda due diligence prinsipining dolzarbligini oshirmoqda.

Due diligence prinsipi xalqaro huquqda davlatlarning o‘z hududidan boshqa davlatlarga zarar yetkazuvchi faoliyatga yo‘l qo‘ymaslik majburiyatini ifodalaydi[2]. Mazkur tamoyil dastlab ekologik huquq va xalqaro xavfsizlik sohalarida qo‘llanilgan bo‘lsa, bugungi kunda u kiberxavfsizlik sohasida ham tobora keng qo‘llanilmoqda.

Kibermakondadue diligence prinsipining qo‘llanilishi davlatlarning xalqaro javobgarligi, xalqaro hamkorlik, davlat suvereniteti va xalqaro xavfsizlik masalalari bilan chambarchas bog‘liqdir. Ayniqsa, transmilliy kiberjinoyatlar va muhim axborot infratuzilmasiga qarshi qaratilgan raqamli hujumlarning ortib borishi ushbu prinsipni xalqaro huquqning muhim elementlaridan biriga aylantirmoqda.

Mazkur tezisning maqsadi due diligence prinsipining xalqaro huquqdagi mazmunini, uning kibermakondagi qo‘llanilishini hamda O‘zbekiston Respublikasi uchun amaliy ahamiyatini tahlil qilishdan iborat.

Due diligence prinsipining xalqaro huquqda shakllanishi. Due diligence prinsipi xalqaro huquqda davlatlarning boshqa davlatlarga zarar yetkazilishining oldini olishga qaratilgan ehtiyotkorlik majburiyatini anglatadi. Mazkur prinsipning shakllanishi XIX asr oxiri va XX asr boshlariga borib taqaladi. Keyinchalik xalqaro sud amaliyoti ushbu tamoyilning rivojlanishiga katta hissa qo‘shdi.

Mazkur prinsipning eng muhim manbalaridan biri Xalqaro sudning 1949-yildagi Korfu bo‘g‘ozi ishidir. Sud o‘z qarorida davlat o‘z hududidan boshqa davlatlarga zarar yetkazuvchi faoliyatga ongli ravishda yo‘l qo‘ymasligi kerakligini ta’kidlagan[3].

Keyinchalik ushbu tamoyil ekologik huquqda ham rivojlandi. 1972-yildagi Stokgolm deklaratsiyasi hamda 1992-yildagi Rio deklaratsiyasida davlatlar o‘z hududidagi faoliyat boshqa davlatlar hududiga zarar yetkazmasligini ta’minlashi lozimligi qayd etilgan[4].

Xalqaro huquq komissiyasining davlatlarning xalqaro-huquqiy javobgarligi to‘g‘risidagi moddalarida ham davlatlarning o‘z majburiyatlarini bajarishi masalasiga alohida e’tibor qaratilgan[5].

[1] UNODC. *Comprehensive Study on Cybercrime*. New York, 2013. P. 221.
[2] Roscini M. *Cyber Operations and the Use of Force in International Law*. Oxford University Press, 2014. P. 89.
[3] Corfu Channel Case (United Kingdom v. Albania), ICJ Reports, 1949. P. 22.
[4] Rio Declaration on Environment and Development, 1992, Principle 2.
[5] International Law Commission. *Articles on Responsibility of States for Internationally Wrongful Acts*, 2001.

So‘nggi yillarda xalqaro huquqshunoslar due diligence prinsipini kiberxavfsizlik sohasiga tatbiq etishni taklif qilmoqdalar. Ularning fikricha, davlat o‘z hududidan boshqa davlatlarga zarar yetkazuvchi kiberoperatsiyalarni amalga oshirishga yo‘l qo‘ymasligi lozim[6].

Due diligence prinsipining kibermakonda qo‘llanilishi. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kibermakon davlatlar o‘rtasidagi munosabatlarning yangi makoniga aylandi. Biroq kibermakondasodir etilayotgan huquqbuzarliklarning aksariyati transchegaraviy xususiyatga ega bo‘lib, ularni aniqlash va ularga huquqiy baho berish an’anaviy xalqaro huquq mexanizmlarini qo‘llashda muayyan qiyinchiliklarni keltirib chiqarmoqda.

Kiberhujumlarning muhim xususiyatlaridan biri ularning anonimligi hisoblanadi. Ko‘plab hollarda hujum bir davlat hududidan turib amalga oshirilgan bo‘lsa-da, hujumni uyushtirgan shaxslar yoki guruhlar boshqa davlat hududida joylashgan bo‘lishi mumkin. Ayrim holatlarda esa davlatlar o‘z hududlarida faoliyat yuritayotgan xakerlik guruhlariga nisbatan yetarli choralar ko‘rmaydi. Natijada kiberhujumlar boshqa davlatlarning axborot infratuzilmasiga jiddiy zarar yetkazishi mumkin.[7]

Shu sababli xalqaro huquqda davlatlarning kibermakondagi majburiyatlarini aniqlash masalasi dolzarb ahamiyat kasb etmoqda. Due diligence prinsipi aynan ushbu muammoni hal qilishga qaratilgan huquqiy mexanizmlardan biri hisoblanadi.

Mazkur prinsipga ko‘ra, davlat o‘z hududi yoki nazorati ostidagi axborot infratuzilmasidan boshqa davlatlarga qarshi zarar yetkazuvchi kiberoperatsiyalar amalga oshirilishining oldini olish uchun barcha zarur choralarni ko‘rishi lozim. Bu yerda davlatning javobgarligi hujumni bevosita amalga oshirganligi bilan emas, balki o‘z hududidan zarar yetkazilishiga yo‘l qo‘yganligi bilan bog‘liq bo‘ladi[7].

Tallinn Manual 2.0 qo‘llanmasining 6-qoidasiga ko‘ra, davlat o‘z hududidan boshqa davlatlarga jiddiy salbiy oqibatlar keltirib chiqaradigan kiberoperatsiyalar amalga oshirilayotganligini bilganda yoki bilishi kerak bo‘lgan hollarda, bunday faoliyatning oldini olish bo‘yicha zarur choralarni ko‘rishi kerak[8].

Mazkur qoida xalqaro huquqshunoslar o‘rtasida keng muhokamalarga sabab bo‘lgan.

Ayrim olimlar due diligence prinsipini xalqaro odat huquqining shakllangan normasi sifatida e’tirof etadilar. Boshqa bir guruh mutaxassislar esa ushbu prinsip hali to‘liq shakllanmaganligini va davlat amaliyoti yetarli emasligini ta’kidlaydilar[9].

Shunga qaramasdan, BMT doirasida olib borilgan muhokamalar va ekspert guruhlari hisobotlari davlatlarning kiberxavfsizlik sohasidagi ehtiyotkorlik majburiyatlari mavjudligini tobora ko‘proq e’tirof etayotganini ko‘rsatmoqda. Xususan, BMT Hukumat ekspertlari guruhi (GGE) hisobotlarida davlatlar o‘z hududidan boshqa davlatlarga zarar yetkazuvchi axborot-kommunikatsiya texnologiyalaridan foydalanilishining oldini olish bo‘yicha choralar ko‘rishi lozimligi qayd etilgan[10].

Due diligence prinsipi amaliy jihatdan bir nechta majburiyatlarni o‘z ichiga oladi. Birinchidan, davlat o‘z axborot infratuzilmasini monitoring qilishi kerak. Ikkinchidan, davlat kiberxavfsizlik hodisalari to‘g‘risidagi ma’lumotlarni yig‘ish va tahlil qilish tizimini yaratishi lozim. Uchinchidan, boshqa davlatlardan kelgan asosli murojaatlar bo‘yicha tegishli choralarni ko‘rishi zarur. To‘rtinchidan, xalqaro hamkorlik mexanizmlarida faol ishtirok etishi talab etiladi[11].

Mazkur prinsip ayniqsa muhim axborot infratuzilmasiga qarshi qaratilgan kiberhujumlar sharoitida alohida ahamiyat kasb etadi. Energetika tizimlari, transport tarmoqlari, bank tizimlari yoki

---

[6] Schmitt M.N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017. Rule 6.

[7] UNODC. *Comprehensive Study on Cybercrime*. New York, 2013. P. 227.

[8] Schmitt M.N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017. Rule 6.

[9] Tsagourias N., Buchan R. *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing, 2015. P. 238.

[10] United Nations Group of Governmental Experts Report, A/70/174, 2015.

[11] Ziolkowski K. *Peacetime Regime for State Activities in Cyberspace*. NATO CCDCOE, 2013. P. 145.

davlat boshqaruvi infratuzilmasiga qarshi amalga oshiriladigan kiberoperatsiyalar nafaqat iqtisodiy zarar keltiradi, balki xalqaro tinchlik va xavfsizlikka ham tahdid solishi mumkin[12].

Kibermakonda due diligence prinsipining qo‘llanilishi davlatlarning xalqaro hamkorligini rivojlantirishga ham xizmat qiladi. Davlatlar o‘rtasida axborot almashish, kiberhodisalar haqida tezkor xabar berish va birgalikdagi choralarni amalga oshirish ushbu tamoyilning amaliy ifodalaridan biri hisoblanadi.

Shu bilan birga, mazkur prinsipni qo‘llashda ayrim muammolar ham mavjud. Xususan, davlatning “bilishi kerak edi” degan mezonni aniqlash, texnik imkoniyatlarning turlicha darajada ekanligi hamda rivojlangan va rivojlanayotgan davlatlar o‘rtasidagi kiber salohiyat tafovutlari amaliyotda murakkabliklarni yuzaga keltirmoqda.

Fikrmizcha, due diligence prinsipining kibermakonda qo‘llanilishi davlatlarning xalqaro javobgarligi va xalqaro hamkorlik o‘rtasidagi muvozanatni ta’minlashga xizmat qiladi. Ushbu tamoyil bir tomondan davlat suverenitetini hurmat qilsa, ikkinchi tomondan davlatlarga o‘z hududidan zarar yetkazilishining oldini olish bo‘yicha aniq majburiyatlar yuklaydi.

Kibermakonda due diligence prinsipining amaliy mazmuni va huquqiy chegaralarini aniqlashda eng muhim manbalardan biri 2017-yilda nashr etilgan *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* hisoblanadi. Mazkur hujjat xalqaro shartnoma maqomiga ega bo‘lmasa-da, xalqaro huquq normalarining kibermakonga tatbiq etilishi bo‘yicha eng nufuzli ilmiy manbalardan biri sifatida e’tirof etiladi.

Qo‘llanmaning 6-qoidasiga ko‘ra, davlat o‘z hududidan boshqa davlatlarga jiddiy zarar yetkazuvchi kiberoperatsiyalar amalga oshirilayotganligini bilganda yoki buni bilishi kerak bo‘lgan hollarda, bunday faoliyatning oldini olish uchun zarur choralarni ko‘rishi lozim[13].

Tallinn Manual ekspertlari ushbu prinsipni xalqaro huquqdagi mavjud odat normalarining kibermakondagi davomiyligi sifatida talqin qiladilar. Ularning fikricha, davlatning javobgarligi har doim ham hujumni bevosita amalga oshirganligi bilan bog‘liq emas. Ayrim hollarda davlatning harakatsizligi yoki yetarli choralar ko‘rmaganligi ham xalqaro javobgarlikka sabab bo‘lishi mumkin[14].

Mazkur masala xalqaro sud amaliyotida ham muhim o‘rin tutadi. Xususan, Korfu bo‘g‘ozi ishida Xalqaro sud davlat o‘z hududidan boshqa davlatlarga zarar yetkazilishiga ongli ravishda yo‘l qo‘ymasligi kerakligini qayd etgan[15].

Garchi ushbu ish kibermakonga bevosita taalluqli bo‘lmasa-da, unda shakllangan yondashuv bugungi kunda kiberxavfsizlik sohasida ham qo‘llanilmoqda.

So‘nggi yillarda davlatlar kiberhujumlarga nisbatan rasmiy pozitsiyalarini ham shakllantira boshladilar. AQSH, Buyuk Britaniya, Avstraliya, Niderlandiya va Fransiya kabi davlatlar o‘zlarining rasmiy huquqiy pozitsiyalarida due diligence prinsipining kibermakonda qo‘llanilishini tan olganlar.

Biroq ayrim davlatlar ushbu prinsipning huquqiy majburiy xarakterga ega ekanligini e’tirof etmasdan, uni siyosiy tavsiya sifatida baholamoqdalar. Shu sababli xalqaro huquqda ushbu masala yuzasidan yakdil yondashuv hali to‘liq shakllanmagan.

BMT doirasida ham davlatlarning kibermakondagi javobgarligi masalalari muntazam muhokama qilinmoqda. Xususan, Hukumat ekspertlari guruhi (GGE) va Ochiq ishchi guruhi (OEWG) hisobotlarida davlatlarning o‘z hududidan boshqa davlatlarga zarar yetkazuvchi axborot-kommunikatsiya texnologiyalaridan foydalanilishiga yo‘l qo‘ymaslik majburiyatlari qayd etilgan.

Mazkur hujjatlar xalqaro hamjamiyatda due diligence prinsipining asta-sekin mustahkamlanib borayotganidan dalolat beradi.

---

[12] Hathaway O.A. et al. The Law of Cyber-Attack. California Law Review. 2012. Vol. 100. P. 870.

[13] Schmitt M.N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017. Rule 6.

[14] Schmitt M.N. *Tallinn Manual 2.0*. Commentary to Rule 6. Cambridge University Press, 2017.

[15] Corfu Channel Case (United Kingdom v. Albania), ICJ Reports, 1949. P. 22.

Kibermakonda due diligence prinsipining qo‘llanilishi O‘zbekiston Respublikasi uchun ham alohida ahamiyatga ega. Mamlakatda raqamlashtirish jarayonlarining jadallashuvi, davlat xizmatlarining elektron shaklga o‘tkazilishi, muhim axborot infratuzilmasi obyektlari sonining ortib borishi kiberxavfsizlik masalalarini milliy xavfsizlikning ustuvor yo‘nalishlaridan biriga aylantirmoqda.

Mamlakatimizda 2022-yilda qabul qilingan “Kiberxavfsizlik to‘g‘risida”gi Qonun milliy kiberxavfsizlik tizimini shakllantirishda muhim huquqiy asos bo‘lib xizmat qilmoqda.

Biroq tadqiqot natijalari shuni ko‘rsatadiki, amaldagi qonunchilikda davlatning xalqaro kiberxavfsizlik majburiyatlari, xususan, due diligence tamoyili alohida mustahkamlanmagan.

Aytish mumkinki, O‘zbekiston Respublikasida mazkur prinsipni bosqichma-bosqich milliy qonunchilikka implementatsiya qilish maqsadga muvofiq hisoblanadi. Bunda davlatning o‘z hududidan boshqa davlatlarga zarar yetkazuvchi kiberfaoliyatning oldini olish, xalqaro axborot almashinuvida ishtirok etish va transmilliy kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlikni rivojlantirish bo‘yicha majburiyatlari belgilanishi lozim.

Shuningdek, muhim axborot infratuzilmasi obyektlarini himoya qilish, milliy CERT markazlari faoliyatini rivojlantirish, xalqaro kiberinsidentlar bo‘yicha axborot almashish mexanizmlarini takomillashtirish ham due diligence prinsipining amaliy ifodasi bo‘lishi mumkin. Bu esa O‘zbekistonning xalqaro kiberxavfsizlik tizimidagi ishtirokini kuchaytirish bilan birga, davlatning xalqaro maydondagi obro‘sini ham mustahkamlaydi.

Xulosa qilib aytganda, due diligence prinsipi zamonaviy xalqaro kiberhuquqning eng muhim institutlaridan biri sifatida shakllanib bormoqda. Ushbu prinsip davlatlarga o‘z hududidan boshqa davlatlarga zarar yetkazuvchi kiberfaoliyatning oldini olish majburiyatini yuklaydi hamda xalqaro hamkorlikni rivojlantirishga xizmat qiladi.

Bugungi kunda kibermakondagi tahdidlarning transmilliy xususiyati xalqaro huquqning an’anaviy tamoyillarini yangi sharoitlarga moslashtirishni talab etmoqda. Shu nuqtai nazardan due diligence prinsipi davlat suvereniteti va xalqaro javobgarlik o‘rtasidagi muvozanatni ta’minlovchi muhim huquqiy mexanizm hisoblanadi.

O‘zbekiston Respublikasi uchun ham mazkur prinsipning amaliy ahamiyati katta bo‘lib, uni milliy qonunchilik va kiberxavfsizlik siyosatiga bosqichma-bosqich joriy etish xalqaro majburiyatlarni samarali bajarish, transmilliy kiberxavflarga qarshi kurashish va xalqaro hamkorlikni rivojlantirishga xizmat qiladi.

Shunday qilib, due diligence prinsipining kibermakonda qo‘llanilishi kelgusida xalqaro huquqning mustaqil va muhim yo‘nalishlaridan biriga aylanishi mumkin. Mazkur tamoyil davlatlarning kibermakondagi xulq-atvorini tartibga solish, xalqaro xavfsizlikni ta’minlash va zamonaviy kiberxavflarga qarshi samarali kurashishning huquqiy asoslaridan biri bo‘lib qoladi.

Foydalanilgan adabiyotlar:

1. Corfu Channel Case (United Kingdom v. Albania), ICJ Reports, 1949.
2. Schmitt M.N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.
3. Roscini M. *Cyber Operations and the Use of Force in International Law*. Oxford University Press, 2014.
4. Shaw M.N. *International Law*. Cambridge University Press, 2021.
5. Tsagourias N., Buchan R. *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing, 2015.
6. United Nations Group of Governmental Experts Report, A/70/174, 2015.
7. United Nations Open-ended Working Group Reports, 2021–2024.

8. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘RQ–764-son, 2022.
9. UNODC. *Comprehensive Study on Cybercrime*. New York, 2013.
10. International Law Commission. *Articles on Responsibility of States for Internationally Wrongful Acts*. 2001.