

KIBERXAVFSIZLIKNI TA'MINLASHNING HUQUQIY MEXANIZMLARI

Jo'rayev Diyorjon

Tashkent international Universiteti

Yurispuridensiya (faoliyat turlari) yo'nalishi talabasi.

<https://doi.org/10.5281/zenodo.19053380>

Annotatsiya. Ushbu maqolada kiberxavfsizlikni ta'minlashning huquqiy mexanizmlari, jumladan, milliy qonunchilik va xalqaro tajriba tahlil qilingan. Raqamli texnologiyalar shiddat bilan rivojlanayotgan bir sharoitda axborot makonida shaxs, jamiyat va davlat manfaatlarini himoya qilishning huquqiy asoslari, sohaga oid mavjud muammolar hamda ularni hal etish istiqbollari ko'rib chiqilgan. Shuningdek, O'zbekiston Respublikasining kiberxavfsizlik sohasidagi qonunchilik bazasi hamda Budapesht konvensiyasi kabi xalqaro hujjatlarning amaliy ahamiyati yoritib berilgan.

Kalit so'zlar: kiberxavfsizlik, huquqiy mexanizmlar, kiberjinoyatchilik, axborot xavfsizligi, milliy qonunchilik, xalqaro huquq, raqamli makon, shaxsga doir ma'lumotlar.

LEGAL MECHANISMS FOR ENSURING CYBERSECURITY

Annotation. This article analyzes the legal mechanisms for ensuring cybersecurity, including national legislation and international experience. In the context of the rapid development of digital technologies, the legal framework for protecting the interests of individuals, society, and the state in the information space, existing problems in the field, and prospects for their resolution are considered. Furthermore, the practical significance of the legislative base of the Republic of Uzbekistan in the field of cybersecurity and international documents such as the Budapest Convention is highlighted.

Keywords: cybersecurity, legal mechanisms, cybercrime, information security, national legislation, international law, digital space, personal data.

KIRISH

XXI asr insoniyat taraqqiyotida tub burilishlar davri sifatida tarixga kirdi. Bu davrning eng yorqin xususiyati shubhasiz axborot-kommunikatsiya texnologiyalarining (AKT) misli ko'rilmagan tezlikda rivojlanishi va hayotimizning barcha jabhalariga chuqur kirib borishidir.

Raqamlashtirish jarayoni iqtisodiyot, davlat boshqaruvi, sog'liqni saqlash, ta'lim, moliya va mudofaa tizimlarini butunlay yangi bosqichga olib chiqdi. Elektron hukumat, elektron tijorat, bulutli texnologiyalar va sun'iy intellekt kabi tushunchalar kundalik hayotimizning ajralmas qismiga aylandi.

Biroq, har qanday buyuk innovatsiya o'zining salbiy oqibatlariga ega bo'lgani kabi, raqamli dunyo ham insoniyat oldiga yangi, kutilmagan tahdidlarni keltirib chiqardi.

Kiberfazo – jismoniy chegaralari mavjud bo'lmagan virtual olam bo'lishiga qaramay, unda sodir bo'layotgan huquqbuzarliklar va jinoyatlar real hayotimizga, jamiyat barqarorligiga hamda davlatning milliy xavfsizligiga o'zining bevosita va vayronkor ta'sirini ko'rsatmoqda.

Kiberxavfsizlik tushunchasi dastlab faqatgina texnik mutaxassislar, dasturchilar va tarmoq muhandislari doirasidagi o'ziga xos tor texnik masala sifatida qabul qilingan.

Dastlabki davrlarda tarmoqlarni himoya qilish uchun antivirus dasturlari, himoya devorlari va shifrlash usullaridan foydalanish yetarli deb hisoblangan.

Ammo vaqt o'tishi bilan amalga oshirilgan kiberhujumlar ko'lami, ma'lumotlar o'g'irlanishi va ularning keltirib chiqarayotgan milliardlab dollarlik iqtisodiy zarari shuni ko'rsatdiki, faqatgina dasturiy hamda texnik yechimlar bilan bu global muammoni hal qilib

bo'lmaydi. Aynan shu nuqtada kiberxavfsizlikni ta'minlashning qat'iy va ishlaydigan huquqiy mexanizmlariga bo'lgan o'tkir zarurat yuzaga keldi.

Huquqiy mexanizmlar jamiyatdagi ijtimoiy munosabatlarni tartibga soluvchi eng kuchli vosita sifatida, kiberfazodagi xatti-harakatlar uchun ham aniq huquq va majburiyatlarni belgilab berishi shart. Davlat axborot tizimlarini himoya qilish, fuqarolarning shaxsga doir ma'lumotlar daxlsizligini ta'minlash, intellektual mulk huquqlarini raqamli makonda muhofaza qilish, va eng asosiysi – kiberjinoyatlarning tarkibini tushunish, ularni huquqiy tasniflash hamda huquqbuzarlarni qonuniy javobgarlikka tortish faqat mukammal qonunchilik bazasi orqaligina amalga oshiriladi.

Kiberjinoyatchilikning o'ziga xos eng murakkab jihati uning transmilliy, ya'ni davlatlararo xarakteridadir. Jinoyatchi bir qit'ada, o'z xonasida kompyuter qarshisida o'tirgan holda, boshqa bir qit'adagi yirik bank tizimiga yoki davlatning strategik obyektlariga qaqshatqich hujum uyushtirishi mumkin. Bu esa o'z navbatida kiberxavfsizlikni huquqiy jihatdan ta'minlashda yagona global yondashuvni, davlatlarning o'zaro huquqiy yordam ko'rsatish to'g'risidagi kelishuvlarini va universal xalqaro shartnomalarni ishlab chiqishni talab etadi.

O'zbekiston Respublikasida ham so'nggi yillarda raqamli iqtisodiyotni rivojlantirish davlat siyosatining ustuvor yo'nalishlaridan biriga aylandi. Barcha sohalarni raqamlashtirish jadal sur'atlarda olib borilayotgan bir paytda, mamlakatimiz axborot va kiberxavfsizlik masalasiga strategik ahamiyat qaratmoqda. Xususan, respublikamizda kiberxavfsizlik sohasidagi tarqoq huquqiy munosabatlarni yaxlit tizimlashtirish va davlat organlarining bu boradagi vakolatlarini aniq belgilab berish maqsadida qabul qilingan qonunchilik hujjatlari soha rivojida muhim qadam bo'ldi.

Mazkur maqolaning maqsadi kiberxavfsizlikni ta'minlashning zamonaviy huquqiy mexanizmlarini, xususan, O'zbekiston milliy qonunchiligidagi mavjud holatni va xalqaro huquqiy tajribani yurisprudensiya nuqtai nazaridan chuqur tahlil qilishdan iborat. Shuningdek, kiberfazoda vujudga kelayotgan huquqiy bo'shliqlarni (kazuslarni) aniqlash, amaliyotdagi muammolarni o'rganish va ularni bartaraf etish yuzasidan ilmiy asoslangan huquqiy yechim va takliflar ishlab chiqish maqolaning asosiy vazifasi etib belgilangan.

ADABIYOTLAR TAHLILI VA METODLAR

Kiberxavfsizlik va axborot makonini huquqiy tartibga solish masalalari so'nggi yillarda mahalliy va xorijiy huquqshunos olimlar tomonidan jadal hamda chuqur o'rganilmoqda. Xorijiy adabiyotlarda kiberjinoyatchilikka qarshi kurashishning xalqaro huquqiy standartlari, xususan, Yevropa Kengashining "Kiberjinoyatchilik to'g'risida"gi (Budapesht, 2001-yil) konvensiyasi qoidalari ko'plab tadqiqotchilar, jumladan, M. Gercke, J. Clough kabi yetakchi huquqshunoslar tomonidan batafsil tahlil qilingan.

Ularning ilmiy asarlarida kiberfazodagi yurisdiksiya muammolari, transmilliy xarakterdagi jinoyatlarni tergov qilish, raqamli dalillarni to'plash, saqlash va davlatlararo huquqiy yordam ko'rsatish masalalari atroflicha yoritilgan. Shuningdek, shaxs daxlsizligi va davlat xavfsizligi o'rtasidagi muvozanatni saqlash masalasi ham xalqaro yurisprudensiyaning diqqat markazida bo'lib kelmoqda.

O'zbekiston milliy yurisprudensiyasida axborot xavfsizligi va kiberxavfsizlikni huquqiy ta'minlash masalalari nisbatan yangi, ammo eng dolzarb tadqiqot obyekti hisoblanadi. Ushbu tadqiqotni olib borish jarayonida asosiy manba sifatida O'zbekiston Respublikasining Konstitutsiyasi, 2022-yil 15-aprelda qabul qilingan "Kiberxavfsizlik to'g'risida"gi, "Shaxsga

doir ma'lumotlar to'g'risida"gi, "Axborotlashtirish to'g'risida"gi va "Elektron hukumat to'g'risida"gi qonunlari asos qilib olindi. Shuningdek, sohada yuzaga kelayotgan o'ziga xos huquqiy bo'shliqlarni o'rganish maqsadida Birlashgan Millatlar Tashkiloti hamda Xalqaro elektraloqa ittifoqi (ITU) hisobotlari, sohaga oid maxsus ilmiy maqolalar, huquqshunos olimlarning dissertatsiyalari, shuningdek, muhim axborot infratuzilmasi obyektlarini himoya qilish bo'yicha mavjud normativ-huquqiy hujjatlar keng tahlilga tortildi. Ushbu yuridik adabiyotlar va qonun hujjatlari kiberxavfsizlikning huquqiy tabiatini anglash hamda tarmoq xavfsizligiga bo'layotgan tahdidlarni huquqiy baholash mexanizmlarini to'liq tushunish uchun poydevor bo'lib xizmat qildi.

Ushbu maqolada qo'yilgan ilmiy maqsad va vazifalarga to'laqonli erishish uchun yurisprudensiyada umumqabul qilingan ilmiy bilishning umumiy, mantiqiy va maxsus huquqiy metodlaridan kompleks tarzda foydalanildi. Tadqiqotning eng asosiy uslubiy negizini axborot texnologiyalari va amaldagi huquq normalari o'rtasidagi dinamik munosabatlarni hamda ularning o'zgaruvchan xususiyatlarini obyektiv o'rganish imkonini beruvchi dialektik bilish metodi tashkil etdi.

Maxsus huquqiy usullardan biri sifatida qiyosiy-huquqiy tahlil metodidan faol foydalanildi. Mazkur metod orqali O'zbekiston Respublikasining kiberxavfsizlikka oid milliy qonunchilik bazasi va ilg'or xorijiy davlatlar tajribasi, xalqaro huquq normalari o'zaro qiyoslandi. Buning natijasida qonunchilikdagi mavjud huquqiy tafovutlar hamda milliy amaliyotga tadbiiq etilishi lozim bo'lgan xorijiy ilg'or yechimlar aniqlandi. Tarixiy-huquqiy metod yordamida mamlakatimizda kiberjinoyatlarga doir qonunchilikning qisqa vaqt ichidagi evolyutsion rivojlanish bosqichlari o'rganib chiqildi.

Shu bilan birga, tizimli-tarkibiy tahlil metodi yordamida kiberxavfsizlikni ta'minlash jarayoni yagona va ko'p qirrali huquqiy tizim sifatida o'rganilib, undagi davlat organlari, xususiy korxonalar va oddiy fuqarolarning uzviy bog'langan huquq hamda majburiyatlari tahlil qilindi.

Huquqbuzarliklarni tasniflash va jinoyat tarkibini aniqlashda formal-yuridik (mantiqiy) metod ustuvorlik qilib, amaldagi normativ-huquqiy hujjatlar matni hamda yuridik atamalarning qonunchilikdagi ifodasi batafsil tahlil qilindi. Global kiberxavfsizlik indeksi kabi ko'rsatkichlarni o'rganishda statistik tahlil, umumiy xulosalar chiqarishda esa induksiya va deduksiya metodlaridan keng foydalanildi. Mazkur yondashuvlar tadqiqot natijalarining ilmiy va amaliy jihatdan yuqori darajada ishonchli ekanligini kafolatlaydi.

NATIJALAR

O'tkazilgan kompleks ilmiy-amaliy tadqiqotlar va amaldagi normativ-huquqiy hujjatlar tahlili shuni ko'rsatdiki, O'zbekiston Respublikasida kiberxavfsizlikni huquqiy ta'minlash borasida so'nggi yillarda inqilobiy o'zgarishlar amalga oshirilgan. Tadqiqotning eng asosiy natijalaridan biri sifatida 2022-yilda "Kiberxavfsizlik to'g'risida"gi Qonunning qabul qilinishini ta'kidlash lozim. Ushbu huquqiy hujjat uzoq yillar davomida turli qonunosti hujjatlarida tarqoq holda mavjud bo'lgan normalarni yagona tizimga keltirdi.

Natijada, O'zbekistonda kiberxavfsizlikni ta'minlash sohasidagi yagona davlat siyosatini amalga oshiruvchi vakolatli organ — Davlat xavfsizlik xizmatining huquqiy maqomi, vazifalari va vakolatlari qat'iy belgilab qo'yildi. Bu esa davlat organlari va xususiy sektor o'rtasida kiberinsidentlarga qarshi tezkor javob qaytarish tizimini huquqiy asosda shakllantirishga xizmat qildi. Tahlil natijalariga ko'ra, milliy huquq tizimida muhim axborot infratuzilmasi (MAI) obyektlarini himoya qilish bo'yicha mutlaqo yangi huquqiy institut yaratilganligi muhim yutuqdir.

Davlat hokimiyati, energetika, moliya, transport, mudofaa va sog'liqni saqlash kabi strategik ahamiyatga ega tizimlar qonun bilan toifalarga ajratildi va ularni davriy huquqiy hamda texnik auditdan o'tkazish majburiyati yuklatildi. Bu amaliyot ehtimoliy kiberhujumlarning davlat milliy xavfsizligiga va iqtisodiyotiga yetkazishi mumkin bo'lgan yirik ko'lamli zararlarining huquqiy oldini olish mexanizmi sifatida ishlay boshladi.

Jinoyat va ma'muriy qonunchilik sohasidagi tadqiqotlar natijalari jazo choralari zamon talablariga moslashtirilganini ko'rsatdi. O'zbekiston Respublikasi Jinoyat kodeksida kompyuter texnikasi vositalaridan foydalanib sodir etiladigan huquqbuzarliklar doirasi kengaytirildi.

Xususan, shaxsga doir ma'lumotlarga qonunga xilof ravishda aralashish (141-2-modda), kompyuter axborotini modifikatsiyalash yoki yo'q qilish, shuningdek, zarar keltiruvchi dasturlarni (viruslar, troyanlar, to'lov talab qiluvchi dasturlar) tarqatish kabi jinoyatlar uchun sanksiyalar og'irlashtirildi. Bu fuqarolarning raqamli makondagi daxlsizlik huquqlarini ishonchli himoya qilish kafolatini kuchaytirdi.

Shunga qaramay, amaliyot va qonunchilik tahlili jarayonida yurisprudensiya nuqtai nazaridan hal qilinishi lozim bo'lgan bir qator jiddiy huquqiy muammolar va bo'shliqlar mavjudligi aniqlandi. Birinchidan, O'zbekiston Respublikasi Jinoyat-protsessual kodeksida "elektron raqamli dalil" (digital evidence) instituti hamda ularni to'plash, protsessual qayd etish, musodara qilish va sud ekspertizasidan o'tkazishning qat'iy mexanizmlari yetarli darajada ochib berilmagan. Ikkinchidan, kiberjinoyatlarning aksariyati transmilliy (chegara bilmas) xarakterga ega ekanligi sababli, yurisdiksiyani belgilashda jiddiy to'siqlar kuzatilmoqda. Jinoyatchi bir davlatda, server boshqa davlatda, jabrlanuvchi esa uchinchi davlatda bo'lgan kazuslarda davlatlararo huquqiy yordam ko'rsatish shartnomalari raqamli tezlikka moslasha olmayapti.

Shuningdek, sun'iy intellekt, blokcheyn va kriptovalyutalar vositasida sodir etilayotgan firibgarlik va o'g'rilik jinoyatlarini to'g'ri huquqiy malakalash borasida sud-tergov amaliyotida yagona yondashuv hali to'liq shakllanmagan.

Ushbu qiyosiy va tahliliy natijalar kiberxavfsizlikni huquqiy ta'minlash faqatgina milliy qonunchilik bilan cheklanib qolmasligini, balki jinoyat qonunchiligini global jarayonlarga moslashtirishni talab etishini isbotlaydi.

MUHOKAMA

Tadqiqot natijalari shuni ko'rsatmoqdaki, O'zbekiston kiberxavfsizlikni huquqiy ta'minlash borasida muhim qadamlarni tashlagan bo'lsa-da, bu jarayon hali o'zining shakllanish va o'tish davrini boshidan kechirmoqda. "Kiberxavfsizlik to'g'risida"gi maxsus qonunning qabul qilinishi yuridik hamjamiyat tomonidan ijobiy baholangan bo'lsa-da, uning ayrim normalari asosan deklarativ xususiyatga ega ekanligi muhokamalarga sabab bo'lmoqda. Qonun to'g'ridan-to'g'ri ishlashi va huquqiy munosabatlarni aniq tartibga solishi uchun o'nlab qonunosti hujjatlari, texnik reglamentlar hamda ko'rsatmalar ishlab chiqilishini talab etadi. Aks holda, qonunda belgilangan vakolatlar va majburiyatlar o'rtasida amaliy kolliziyalar (qarama-qarshiliklar) yuzaga kelish xavfi saqlanib qoladi.

Bundan tashqari, kiberjinoyatchilikning mutlaqo chegarasiz va transmilliy tabiati faqatgina milliy qonunchilik bilan bu muammoni hal qilib bo'lmasligini isbotlamoqda. Shu o'rinda, xalqaro huquqiy tajriba, xususan, Yevropa Kengashining Kiberjinoyatchilik to'g'risidagi (Budapesht, 2001) konvensiyasi qoidalari bilan milliy qonunchilikni uyg'unlashtirish masalasi dolzarbdir. Garchi mamlakatimiz ushbu konvensiyaga to'liq qo'shilmagan bo'lsa ham, undagi kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni ushlash, raqamli firibgarlik kabi jinoyat tarkiblarini milliy Jinoyat kodeksiga to'liq implementatsiya qilish yuridik zaruratdir.

Shuningdek, xalqaro hamkorlik doirasida kiberhujumlar bo'yicha tezkor ma'lumot almashish uchun 24/7 rejimida ishlovchi davlatlararo aloqa tarmoqlarini huquqiy jihatdan mustahkamlash talab etiladi.

Natijalar qismida qayd etilganidek, eng jiddiy huquqiy bo'shliq moddiy huquqda emas, balki jinoyat-protsessual huquqida namoyon bo'lmoqda. "Elektron raqamli dalil"larning (IP manzillar, server log-fayllari, elektron yozishmalar, blokcheyn tranzaksiyalari) yuridik kuchga ega bo'lishi uchun ularni to'plash, qayd etish va saqlashning aniq protsessual mexanizmlari amaldagi Jinoyat-protsessual kodeksida to'laqonli o'z aksini topmagan.

Bulutli texnologiyalarda (cloud computing) saqlanayotgan ma'lumotlarni tergov qilishda qaysi davlat yurisdiksiyasi amal qilishi yoki kriptovalyuta orqali amalga oshirilgan huquqbuzarliklarda raqamli aktivlarni xatlashning huquqiy asoslari noaniqligicha qolmoqda. Bu an'anaviy ashyoviy dalillarga asoslangan tergov usullarini virtual makon spetsifikasiga tezroq moslashtirishni taqozo qiladi.

Yana bir muhim muhokama obyekti — bu innovatsion texnologiyalar va sun'iy intellekt (SI) yordamida sodir etilayotgan huquqbuzarliklardir. Amaldagi huquqiy normalar faqat inson tomonidan sodir etilgan jinoyatlarga moslashtirilgan.

Ammo huquqbuzarlik avtonom ishlovchi SI algoritmi tomonidan sodir etilsa, yuridik javobgarlik subyekti kim bo'ladi: dastur yaratuvchisi, foydalanuvchisi yoki SI tizimining o'zimi? Ushbu huquqiy kazus kelajak yurisprudensiyasining eng katta sinovlaridan biri bo'lishi shubhasiz.

Yakuniy va eng nozik masala bu — kiberxavfsizlik choralari va insonning fundamental huquqlari o'rtasidagi oltin muvozanatni saqlashdir. Davlat tomonidan axborot xavfsizligini ta'minlash maqsadida internet makoni ustidan nazoratning kuchaytirilishi fuqarolarning so'z erkinligi hamda shaxsiy hayot daxlsizligi huquqlariga putur yetkazmasligi shart. Xulosa qilib aytganda, kiberxavfsizlikning huquqiy mexanizmlari faqatgina jazolovchi va taqiqlovchi xarakterda bo'lib qolmasdan, balki demokratik tamoyillarga asoslangan holda raqamli huquqlarni himoya qiluvchi asosiy qalqon vazifasini o'tashi lozim.

XULOSA

Xulosa o'rnida shuni ta'kidlash joizki, kiberxavfsizlikni huquqiy jihatdan ta'minlash bugungi shiddatli raqamli davrning eng ustuvor va kechiktirib bo'lmaydigan vazifalaridan biriga aylandi. O'tkazilgan huquqiy tahlillar shuni yaqqol ko'rsatmoqdaki, O'zbekiston Respublikasida kiberfazo daxlsizligini saqlash va axborot infratuzilmalarini himoya qilish bo'yicha mustahkam huquqiy poydevor yaratilmoqda.

Xususan, "Kiberxavfsizlik to'g'risida"gi qonunning qabul qilinishi sohada yagona davlat siyosatini tizimlashtirish hamda ishtirokchilarning huquq va majburiyatlarini qat'iy belgilashga xizmat qildi.

Biroq, texnologiyalarning to'xtovsiz rivojlanishi, kiberjinoyatlarning misli ko'rilmagan tezkor evolyutsiyasi va ularning o'ta transmilliy xarakteri milliy qonunchilikni ham doimiy ravishda, davr talabiga mos ravishda takomillashtirib borishni talab etadi. Muhokama jarayonida aniqlangan asosiy muammolardan biri – jinoyat-protsessual huquqida "elektron raqamli dalillar" bilan ishlash mexanizmlarining yetarli darajada tartibga solinmaganligidir.

Ushbu huquqiy bo'shliqni bartaraf etish maqsadida amaldagi Jinoyat-protsessual kodeksiga raqamli dalillarni yig'ish, qayd etish, xatlash va huquqiy baholashning aniq protsessual tartibini belgilovchi maxsus normalar kiritish taklif etiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Gulyamov S. S., Rustambekov I. R. Axborot va kiberxavfsizlikning huquqiy asoslari : o'quv qo'llanma / S. S. Gulyamov, I. R. Rustambekov. – Toshkent : TDYU nashriyoti, 2021. – 250 b.
2. Rustamboyev M. H. O'zbekiston Respublikasi Jinoyat huquqi. Maxsus qism : darslik / M. H. Rustamboyev. – Toshkent : "Yuridik adabiyotlar publish", 2021. – 688 b.
3. Рассолов И. М. Информационное право : учебник для вузов / И. М. Рассолов. – 5-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2020. – 347 с.
4. Clough J. Principles of Cybercrime / J. Clough. – 2nd ed. – Cambridge : Cambridge University Press, 2015. – 480 p.
5. Xalilov A. A. Kiberxavfsizlikni ta'minlashda milliy qonunchilik va xalqaro standartlar integratsiyasi // Huquq va burch jurnali. – Toshkent, 2022. – № 4. – B. 34-39.
6. Okyulov O. Raqamli iqtisodiyot va axborot xavfsizligi masalalarining huquqiy tahlili // Yuridik fanlar axborotnomasi. – Toshkent, 2020. – № 2. – B. 112-118.