KIBERXAVFSIZLIKNI OLDINI OLISHGA QARATILGAN HUQUQIY MEZONLAR

I.A. Ismoilov
Farg'ona davlat universiteti, falsafa fanlari bo'yicha falsafa doktori (PhD)
Abduxalilova Nasibaxon Farhod qizi
Farg'ona davlat universiteti talabasi

Annotatsiya: Mazkur maqolada kiberxavfsizlikni ta'minlash va kiberjinoyatlarning oldini olishga qaratilgan huquqiy mezonlar tahlil qilinadi. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida yuzaga kelayotgan kiberxavflar — shaxsiy ma'lumotlarning noqonuniy tarqalishi, elektron firibgarlik va axborot tizimlariga ruxsatsiz kirish kabi tahdidlarning huquqiy jihatlari o'rganiladi. O'zbekiston Respublikasining kiberxavfsizlik sohasidagi qonunchiligi va xalqaro tajriba taqqoslab tahlil qilinadi.

Kalit so'zlar: kiberxavfsizlik, kiberjinoyat, huquqiy mezonlar, axborot xavfsizligi, shaxsiy ma'lumotlar, Legal Tech, raqamlashtirish.

Аннотация: В данной статье анализируются правовые критерии обеспечения кибербезопасности и предотвращения киберпреступлений. Изучаются правовые аспекты киберугроз: незаконное распространение персональных данных, электронное мошенничество, несанкционированный доступ к информационным системам. Проводится сравнительный анализ законодательства Республики Узбекистан в области кибербезопасности и международного опыта.

Ключевые слова: кибербезопасность, киберпреступность, правовые критерии, информационная безопасность, персональные данные, юридические технологии, цифровизация.

Bugungi raqamli asrda axborot-kommunikatsiya texnologiyalarining shiddat bilan rivojlanishi insoniyat hayotining barcha sohalarini o'zgartirib yubormoqda. Biroq bu jarayon bilan parallel ravishda kibertahdidlar ham keskin ortib bormoqda. Ichki ishlar vazirligi ma'lumotlariga ko'ra, 2019-yilda 863 ta kiberjinoyat qayd etilgan bo'lsa, 2024-yilda bu ko'rsatkich 58,8 mingtaga yetdi — kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 6,2%dan 44,4%ga ko'tarildi.[1] Bu statistika kiberxavfsizlikni huquqiy tartibga solishning nafaqat texnik, balki ijtimoiy-huquqiy muammo ekanini ko'rsatadi.

[1]Ichki ishlar vazirligi statistikasi: 2019–2024-yillar bo'yicha kiberjinoyatlar dinamikasi.

O'zbekistonda raqamli transformatsiya jadal amalga oshirilayotgan bir sharoitda kiberxavfsizlikni ta'minlashga qaratilgan huquqiy mezonlarni tahlil qilish va takomillashtirish **dolzarb ilmiy-amaliy masala** bo'lib qolmoqda. Mavzuning ahamiyati quyidagilarda namoyon bo'ladi: shaxsiy ma'lumotlarni himoya qilish zarurati; davlat axborot tizimlarining xavfsizligi; raqamli iqtisodiyotga bo'lgan ishonchni mustahkamlash; xalqaro kiber-hamkorlikni rivojlantirish.

Mavzuning o'rganilganlik darajasi

Kiberxavfsizlikning huquqiy jihatlari xalqaro adabiyotda keng yoritilgan bo'lsa-da, O'zbekiston milliy kontekstida tadqiqotlar hali shakllanish bosqichida. Xalqaro darajada kiberxavfsizlik huquqi sohasida Europol, UNODC va Budapesht konvensiyasi[2] doirasida keng ilmiy bazis to'plangan. Milliy qonunchilik tahlilida esa 2022-yilda qabul qilingan «Kiberxavfsizlik to'g'risida»gi Qonun[3] va 2024-yildagi O'RQ-964-son Qonun[4] muhim me'yoriy-huquqiy asos bo'lib xizmat qilmoqda.

Mahalliy tadqiqotchilar orasida huquq-axborot texnologiyalari kesishmasidagi masalalar hali yetarlicha o'rganilmagan. Xususan, kriptoaktivlar bilan bog'liq kiberjinoyatlarni kvalifikatsiya qilish, blokcheyn-asoratlardagi huquqiy bo'shliqlar, hamda Jinoyat kodeksining XXI bobidagi sanksiyalarning yetarliligi yuzasidan maxsus monografik tadqiqotlar mavjud emas.

Tadqiqot metodologiyasi

Tadqiqotda quyidagi ilmiy usullardan foydalanildi:

— taqqoslama-huquqiy tahlil: O'zbekiston qonunchiligi va xalqaro standartlarni (Budapest Convention, EU NIS2 Directive) qiyoslash;

— empirik usul: IIV statistik ma'lumotlarini o'rganish va tendentsiyalarni aniqlash;

— me'yoriy-huquqiy tahlil: Jinoyat kodeksining 278^2, 278^4-moddalari va Prezident qarorlarini kontekstual o'rganish;

— tizimli yondashuv: kiberxavfsizlikni huquqiy, texnik va ijtimoiy jihatlarining o'zaro bog'liqligi nuqtai nazaridan baholash.

4. Asosiy tahlil va natijalar

4.1. Milliy qonunchilik holati

O'zbekiston Respublikasi Jinoyat kodeksining XXI bobi[5] axborot texnologiyalari orqali sodir etiladigan jinoyatlarni huquqiy jihatdan tartibga soladi. 278^2-modda bo'yicha «kompyuter axborotidan ruxsatsiz foydalanish» jinoyati bazaviy hisoblash miqdorining yuz baravarigacha jarima yoki uch yilgacha muayyan huquqdan mahrum

[2]Budapesht konvensiyasi (Convention on Cybercrime), 23.11.2001. – UNODC.
[3]O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni (O'RQ-764-son, 15.04.2022). – CSEC.uz.
[4]O'zbekiston Respublikasining "Kiberxavfsizlikni ta'minlash sohasidagi qonunchilik takomillashtirilishi munosabati bilan ayrim qonun hujjatlariga o'zgartish va qo'shimchalar kiritish to'g'risida"gi Qonuni (O'RQ-964-son, 20.09.2024). – Lex.uz.
[5]O'zbekiston Respublikasining Jinoyat kodeksi. Maxsus qism, XX1 bob. – Lex.uz.

qilish bilan jazolanadi. 278⁴-modda esa «kompyuter axborotini modifikatsiyalash» jinoyati uchun ikki yilgacha ozodlikdan mahrum qilishni nazarda tutadi.

2022-yilda qabul qilingan «Kiberxavfsizlik to'g'risida»gi Qonun[6] davlat organlari, yuridik va jismoniy shaxslarning axborot xavfsizligi sohasidagi huquq va majburiyatlarini belgiladi. 2024-yilgi O'RQ-964-son Qonun[7] esa sanksiyalar tizimini yanada kuchaytirdi va kiberjinoyat uchun javobgarlikni og'irlashtirishga qaratilgan yangi normalarni joriy etdi.

4.2. Huquqiy tartibga solishdagi muammolar

Amaliyotda bir qator tizimli muammolar aniqlangan. Birinchidan, kriptoaktivlar va blokcheyn bilan bog'liq kiberjinoyatlarni kvalifikatsiya qilishda qonunchilik bo'shliqlari mavjud. Sudlar ushbu holatlarni Jinoyat kodeksining qaysi normasi bilan to'g'ri kvaifikatsiya qilish masalasida qiyinchiliklarga duch kelmoqda. Ikkinchidan, elektron isbotlar (elektron izlar, skrinshot, loglar) dan sudlov amaliyotida foydalanish tartibi to'liq tartibga solinmagan.

2024-yil 30-apreldagi Prezident qarori[8] kiberjinoyatlarga qarshi kurashish tizimini takomillashtirishga qaratilgan bo'lsada, markazlashgan koordinatsiya mexanizmi va moliyaviy razvedka institutlari o'rtasidagi real-time ma'lumot almashinuvi tizimi hali to'liq shakllanmagan. Bu holat kiberjinoyatlarning tezkor aniqlash va ularni huquqiy jihatdan bartaraf etishni qiyinlashtirmoqda.

Xalqaro tajriba va O'zbekistonning o'rni

Budapesht konvensiyasi[9] 65 dan ortiq davlat tomonidan ratifikatsiya qilingan bo'lib, kiberxavfsizlik sohasidagi xalqaro huquqning asosiy manbasi hisoblanadi. Konvensiya doirasida davlatlar o'rtasida operativ ma'lumot almashish, jinoyatchilarni ekstraditsiya qilish va raqamli isbotlarni tan olish mexanizmlari o'rnatilgan. O'zbekistonga ushbu konvensiyaga qo'shilish, xalqaro CERT tarmoqlariga a'zo bo'lish hamda INTERPOL Cybercrime direksiyasi bilan hamkorlikni kuchaytirish tavsiya etiladi.

Muallif fikrlari va tavsiyalar

Tadqiqot natijalari asosida quyidagi ilmiy-amaliy xulosalar va tavsiyalar ishlab chiqildi:

1. **Qonunchilikni takomillashtirish:** Jinoyat kodeksiga axborot texnologiyalari orqali sodir etiladigan jinoyatlar uchun muqobil sanksiyalar — kiberxizmatlardan mahrum qilish, aktivlarni muzlatish — qo'shish zarur.

[6] O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni (O'RQ-764-son, 15.04.2022). – CSEC.uz
[7] O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni (O'RQ-764-son, 15.04.2022). – CSEC.uz
[8]O'zbekiston Respublikasi Prezidentining 2024-yil 30-apreldagi qarori. "Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga qarshi kurashish tizimini takomillashtirish chora-tadbirlari to'g'risida". – CBU.uz.

Kriptoaktivlar va NFT bilan bog'liq jinoyatlarni alohida kvalifikatsiya qiluvchi normalar kiritilishi lozim.

2. **Institutsional mustahkamlash:** Ichki ishlar vazirligi, Markaziy bank, Davlat soliq qo'mitasi va CSEC o'rtasida doimiy koordinatsiya markazi tashkil etish. Real-time kibertahdid monitoringi tizimini joriy etish.

3. **Moliyaviy himoya:** Banklar va to'lov tizimlarida antifrod mexanizmlarini majburiy joriy etish standartlarini belgilash. Kiber-sug'urta institutini huquqiy asoslash va rivojlantirish.

4. **Kadrlar salohiyati:** Huquqshunoslar va tergovchilarni raqamli forensik ekspertiza bo'yicha ixtisoslashtirilgan o'qitish dasturlarini ishlab chiqish. Sudlov amaliyotida elektron isbotlarni qabul qilish tartibi to'g'risida plenumi qarorlarini yangilash.

5. **Aholi savodxonligi:** Ta'lim muassasalarida kiberxavfsizlik darslarini joriy etish; ommaviy ma'lumot berishda davlat va xususiy sektor hamkorligini yo'lga qo'yish.

Xulosa

Kiberxavfsizlik bugungi axborot asrida yirik ijtimoiy-huquqiy muammo sifatida o'z mohiyatini tobora kuchaytirmoqda. Tadqiqot shuni ko'rsatadiki, O'zbekiston raqamli transformatsiya sharoitida milliy kiberxavfsizlik qonunchiligini sezilarli darajada rivojlantirishga erishgan. Biroq amaliyotdagi bo'shliqlar — kriptoaktivlar bilan bog'liq jinoyatlar kvalifikatsiyasi, koordinatsiya mexanizmlari zaifligi, elektron isbotlar tartibi noaniqligini — bartaraf etish uchun tizimli yondashuv talab etiladi.

Faqatgina qonunchilik, texnologiya, ta'lim va xalqaro hamkorlikning uyg'un rivojlanishi orqali kibertahdidlarga qarshi samarali tizim barpo etish mumkin. Ushbu tadqiqot natijalari kiberxavfsizlik sohasidagi keyingi qonun islohotlari uchun ilmiy asos bo'lib xizmat qilishi mumkin.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasining Jinoyat kodeksi. Maxsus qism, XX1 bob. – Lex.uz.

2. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni (O'RQ-764-son, 15.04.2022). – CSEC.uz.

3. O'zbekiston Respublikasi Prezidentining 2024-yil 30-apreldagi "Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga qarshi kurashish tizimini takomillashtirish chora-tadbirlari to'g'risida"gi qarori. – CBU.uz.

4. O'zbekiston Respublikasining "Kiberxavfsizlikni ta'minlash sohasidagi qonunchilik takomillashtirilishi munosabati bilan ayrim qonun hujjatlariga o'zgartish va qo'shimchalar kiritish to'g'risida"gi Qonuni (O'RQ-964-son, 20.09.2024). – Lex.uz.

5. Budapesht konvensiyasi (Convention on Cybercrime), 23.11.2001. – UNODC.

6. Ichki ishlar vazirligi statistikasi: 2019–2024-yillar bo'yicha kiberjinoyatlar dinamikasi.