



INTERNATIONAL LEGAL AND NATIONAL MECHANISMS FOR COMBATING CYBERCRIME: CHALLENGES AND DEVELOPMENT PROSPECTS

Abdullayev Sunnat Nurulla o'g'li

Second-year student in the Jurisprudence program at Sarbon University

Murtazoyeva Sarvara Ma'ruf qizi

First-year student in the Jurisprudence program at Sarbon University

Abstract

The article analyzes the legal foundations for combating cybercrime in the Republic of Uzbekistan and international approaches to this issue. The aim of the study is to identify how cybersecurity, personal data protection, electronic evidence, and international cooperation are regulated under national legislation and foreign legal instruments. Systematic legal and comparative analysis methods are employed. The findings substantiate the need to improve the practical application of legal norms, ensure the integrity of electronic evidence, and coordinate cross-border cooperation. The authors propose developing a unified procedural approach to handling electronic evidence, strengthening interagency cooperation, and increasing public digital literacy.

Keywords

cybercrime, cybersecurity, cyberspace, personal data, electronic evidence, international cooperation, national legislation, comparative legal analysis.

KIBERJINOYATCHILIKKA QARSHI KURASHISHNING XALQARO- HUQUQIY VA MILLIY MEKANIZMLARI: MUAMMOLAR VA RIVOJLANISH ISTIQBOLLARI

Abdullayev Sunnat Nurulla o'g'li

Sarbon universiteti, "Yurisprudensiya" ta'lim yo'nalishi, 2-bosqich talabasi

Murtazoyeva Sarvara Ma'ruf qizi

Sarbon universiteti, "Yurisprudensiya" ta'lim yo'nalishi, 1-bosqich talabasi



Annotatsiya. Maqolada kiberjinoyatchilikka qarshi kurashishning O‘zbekiston Respublikasidagi huquqiy asoslari va xalqaro yondashuvlar tahlil qilinadi. Tadqiqotning maqsadi milliy qonunchilik hamda xorijiy huquqiy hujjatlarda kiberxavfsizlik, shaxsga doir ma’lumotlarni himoya qilish, elektron dalillar va xalqaro hamkorlik masalalari qanday tartibga solinishini aniqlashdan iborat. Tizimli-huquqiy va qiyosiy tahlil usullaridan foydalanildi. Tahlil natijasida huquqiy normalarni amaliy qo‘llash, elektron dalillarning yaxlitligini ta’minlash va transchegaraviy hamkorlikni muvofiqlashtirishni takomillashtirish zarurligi asoslandi. Mualliflar elektron dalillar bilan ishlash bo‘yicha yagona protsessual yondashuvni ishlab chiqish, idoralararo hamkorlikni kuchaytirish hamda aholining raqamli savodxonligini oshirish yuzasidan takliflar berilgan.

Kalit so‘zlar: kiberjinoyatchilik, kiberxavfsizlik, kibernakon, shaxsga doir ma’lumotlar, elektron dalillar, xalqaro hamkorlik, milliy qonunchilik, qiyosiy-huquqiy tahlil.

Kirish. Raqamli texnologiyalarning rivojlanishi davlat boshqaruvi, iqtisodiyot, ta’lim, bank-moliya va kundalik muloqotda yangi imkoniyatlar yaratmoqda. Shu bilan birga, axborot tizimlaridan noqonuniy foydalanish, hisob yozuvlarini egallab olish, fishing, zararli dasturlarni tarqatish va shaxsga doir ma’lumotlarni noqonuniy qayta ishlash kabi xatti-harakatlar huquqni muhofaza qilish organlari oldiga yangi vazifalarni qo‘ymoqda. Kiberjinoyatlarning o‘ziga xos tomoni shundaki, jinoyat sodir etuvchi, jabrlanuvchi, server va elektron dalillar turli davlatlarda joylashgan bo‘lishi mumkin. Shu sababli jinoyatni aniqlash va tergov qilishda yurisdiksiya, dalillarni tezkor saqlash, qonuniy olish va davlatlararo huquqiy yordam muhim ahamiyat kasb etadi.

O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi munosabatlar, jumladan, “Kiberxavfsizlik to‘g‘risida”gi Qonun, “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun va Jinoyat kodeksining axborot texnologiyalari sohasidagi jinoyatlarga oid normalari orqali tartibga solinadi. Ushbu hujjatlar bir-birini to‘ldiradi: maxsus qonunlar himoya va boshqaruv talablarini belgilasa, Jinoyat kodeksi muayyan qilmishlar uchun jinoiy javobgarlik asoslarini belgilaydi. Biroq qonunchilikning samaradorligi faqat norma mavjudligi bilan emas, balki uning amalda izchil qo‘llanishi, texnik imkoniyatlar va



idoralararo hamkorlik bilan ham belgilanadi.

Maqolaning maqsadi kiberjinoyatchilikka qarshi kurashishning milliy-huquqiy asoslarini xalqaro va ayrim xorijiy davlatlar tajribasi bilan qiyoslash, dolzarb muammolarni ajratish hamda takomillashtirish bo'yicha asoslangan takliflar ishlab chiqishdan iborat. Tadqiqotning amaliy ahamiyati elektron dalillar bilan ishlash va transchegaraviy hamkorlikka oid tavsiyalarni tizimlashtirishda namoyon bo'ladi.

Adabiyotlar tahlili. Kiberjinoyatchilikka qarshi kurashishning milliy huquqiy asoslarini o'rganishda, avvalo, O'zbekiston Respublikasi Konstitutsiyasi muhim ahamiyatga ega. Konstitutsiyada shaxsiy hayot daxlsizligi, yozishmalar va boshqa xabarlar sirini saqlash, shuningdek, axborot izlash, olish va tarqatish huquqlariga oid kafolatlar belgilangan. Ushbu normalar raqamli muhitda inson huquq va erkinliklarini himoya qilishning konstitutsiyaviy asoslarini tashkil etadi [1].

O'zbekiston Respublikasining 2022-yil 15-apreldagi O'RQ-764-son "Kiberxavfsizlik to'g'risida"gi Qonuni kiberxavfsizlik sohasidagi munosabatlarni tartibga solishning asosiy huquqiy manbalaridan biridir. Mazkur qonun kiberxavfsizlikni ta'minlash, tegishli subyektlarning vakolatlarini belgilash va axborot tizimlarini himoya qilishga oid munosabatlarni huquqiy jihatdan tartibga soladi [2].

O'zbekiston Respublikasining 2019-yil 2-iyuldagi O'RQ-547-son "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni shaxsga doir ma'lumotlarni yig'ish, saqlash, qayta ishlash va himoya qilish bilan bog'liq munosabatlarni tartibga soladi. Kiberjinoyatchilik sharoitida mazkur qonun fuqarolarning shaxsiy ma'lumotlarini noqonuniy foydalanishdan himoya qilish nuqtayi nazaridan alohida ahamiyatga ega [3].

Kiberjinoyatlarning jinoiy-huquqiy asoslari O'zbekiston Respublikasi Jinoyat kodeksida mustahkamlangan. Xususan, kodeksning axborot texnologiyalari sohasidagi jinoyatlarga bag'ishlangan XX¹ bobi axborotlashtirish qoidalarini buzish, kompyuter axborotidan ruxsatsiz foydalanish va boshqa tegishli qilmishlar uchun jinoiy javobgarlikni nazarda tutadi [4].

O'zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-son "Axborotlashtirish



to'g'risida"gi Qonuni axborotlashtirish sohasidagi munosabatlarni tartibga soluvchi huquqiy manbalardan biridir. Ushbu qonun axborot resurslari va axborot tizimlari bilan bog'liq munosabatlarning huquqiy asoslarini belgilash orqali raqamli muhit xavfsizligini ta'minlashga doir qonunchilik tizimini to'ldiradi [5].

Xalqaro miqyosda Yevropa Kengashining 2001-yil 23-noyabrdagi Kiberjinoyatchilik to'g'risidagi konvensiyasi, ya'ni Budapesht konvensiyasi muhim huquqiy manba hisoblanadi. Konvensiyada kiberjinoyatlarni milliy qonunchilikda belgilash, protsessual vakolatlar va xalqaro hamkorlik masalalari yoritilgan. O'zbekistonning ushbu konvensiyaga nisbatan huquqiy maqomi rasmiy ishtirokchilar ro'yxati asosida baholanishi lozim. Shu sababli konvensiya maqolada qiyosiy-huquqiy tahlil manbasi sifatida ko'rib chiqiladi [6].

Kiberjinoyatchilikka qarshi kurashishda ma'muriy-huquqiy mexanizmlar ham muhim o'rin tutadi. O'zbekiston Respublikasining Ma'muriy javobgarlik to'g'risidagi kodeksi tegishli huquqbuzarliklar uchun ma'muriy javobgarlikni belgilashda ahamiyatga ega. Mazkur hujjatning maqola mavzusiga daxldor normalarini tahlil qilish kiberxavfsizlik sohasidagi huquqiy javobgarlik tizimini kengroq yoritish imkonini beradi [7].

Raqamli davlat xizmatlari va elektron hujjatlar bilan bog'liq munosabatlarni tartibga solishda O'zbekiston Respublikasining 2015-yil 9-dekabrdagi O'RQ-395-son "Elektron hukumat to'g'risida"gi Qonuni muhim ahamiyatga ega. Ushbu hujjat elektron davlat xizmatlarini ko'rsatish va elektron hukumat tizimining huquqiy asoslarini belgilaydi [8].

Shuningdek, O'zbekiston Respublikasining 2022-yil 12-oktabrdagi O'RQ-793-son "Elektron raqamli imzo to'g'risida"gi Qonuni elektron hujjatlarning haqiqiylikini tasdiqlash va elektron raqamli imzodan foydalanish bilan bog'liq munosabatlarni tartibga soladi. Ushbu huquqiy mexanizmlar elektron hujjatlar bilan ishlashda ishonchlilik va axborot xavfsizligini ta'minlash nuqtayi nazaridan ahamiyatlidir [9].

Xorijiy tajribani qiyosiy o'rganishda AQShning Computer Fraud and Abuse Act hujjati kompyuter tizimlariga ruxsatsiz kirish va tegishli xatti-harakatlarni tartibga solish jihatidan ahamiyatlidir [10]. Buyuk Britaniyaning Computer Misuse Act 1990 hujjati



ham kompyuter tizimlaridan ruxsatsiz foydalanishga qarshi kurashishning huquqiy asoslarini belgilaydi [11].

Yevropa Ittifoqining 2016/679-sonli Umumiy ma'lumotlarni himoya qilish reglamenti (GDPR) shaxsga doir ma'lumotlarni qayta ishlash, ma'lumotlar subyektlarining huquqlari va ma'lumotlar xavfsizligiga oid talablarni belgilaydi [12]. Singapurning Cybersecurity Act 2018 hujjati esa kiberxavfsizlikni ta'minlash va muhim axborot tizimlarini himoya qilishga qaratilgan huquqiy mexanizmlarni nazarda tutadi [13].

Yaponiyaning ruxsatsiz kompyuterga kirishni taqiqlashga oid qonuni ham kompyuter tizimlariga noqonuniy kirish bilan bog'liq qilmishlarni tartibga solish nuqtayi nazaridan qiyosiy tahlil uchun ahamiyatli hisoblanadi [14].

Kiberjinoyatchilikka qarshi kurashishning dolzarbligini yoritishda O'zbekiston Respublikasi Hukumat portalida e'lon qilingan kiberjinoyatlarning oldini olish va zamonaviy tahdidlarga qarshi kurashish masalalariga oid axborot materiallari ham qo'shimcha manba bo'lib xizmat qiladi [15]. Yuqoridagi manbalar tahlili kiberjinoyatchilikka qarshi kurashish ko'p yo'nalishli huquqiy yondashuvni talab etishini ko'rsatadi. Milliy qonunchilik jinoiy va ma'muriy javobgarlik, axborot tizimlarini himoya qilish hamda shaxsga doir ma'lumotlar xavfsizligini tartibga solsa, xalqaro va xorijiy hujjatlar kiberjinoyatlarni tergov qilish, ma'lumotlarni himoya qilish va xalqaro hamkorlik mexanizmlarini qiyosiy baholash imkonini beradi.

Metodologiya. Tadqiqotda tizimli-huquqiy tahlil, qiyosiy-huquqiy tahlil va normativ hujjatlarni mazmunan o'rganish usullaridan foydalanildi. Tizimli tahlil orqali milliy huquqiy manbalarning o'zaro aloqasi ko'rib chiqildi. Qiyosiy-huquqiy tahlilda quyidagi mezonlar qo'llandi: 1.Kiberjinoyatlarni taqiqlash va javobgarlik belgilash; 2.Axborot tizimlari hamda muhim infratuzilmani himoya qilish; 3.Elektron dalillarni olish, saqlash va sudga baholash; 4.Shaxsiy hayot va ma'lumotlar himoyasi; 5.Davlatlararo huquqiy hamkorlik. Statistik qismda O'zbekiston hukumat portalida e'lon qilingan, 2019 va 2024-yillardagi axborot texnologiyalari orqali sodir etilgan jinoyatlar haqidagi ma'lumotlar sifatida olingan.



Tahlil va natijalar. O‘zbekiston hukumat portalida e’lon qilingan ma’lumotga ko‘ra, 2019-yilda axborot texnologiyalari orqali 863 ta jinoyat qayd etilgan, 2024-yilda esa bu ko‘rsatkich 58 800 tani tashkil etgan. Shu manbada 2019–2024-yillar oralig‘ida bunday jinoyatlar soni sezilarli oshgani va fuqarolarga katta miqdorda moddiy zarar yetkazilgani qayd etiladi. Ushbu ma’lumotlar kiberjinoyatchilikka qarshi kurashishning dolzarbligini ko‘rsatadi. Biroq statistik raqamlar qiyoslanganda hisobga olish uslubidagi o‘zgarishlar, jinoyatlarni tasniflash va qayd etish amaliyoti ham natijaga ta’sir qilishi mumkin. Shu sababli faqat raqamlarning o‘lishiga asoslanib sabab-oqibat haqida qat’iy xulosa chiqarish to‘g‘ri emas. Milliy mexanizmlarning kuchli jihati — kiberxavfsizlik, shaxsga doir ma’lumotlar va jinoiy javobgarlikni tartibga soluvchi bir nechta normativ-huquqiy manbaning mavjudligidir. “Elektron hukumat to‘g‘risida”gi va elektron raqamli imzoga oid qonunchilik raqamli xizmatlar hamda elektron hujjatlar muhitining huquqiy asoslarini to‘ldiradi. Muammo esa turli normalarning amaliy qo‘llanishi va texnik jarayonlar bilan uyg‘unlashuvida yuzaga kelishi mumkin. Masalan, elektron dalil sifatida ishlatiladigan fayl, server jurnali yoki elektron yozishma o‘zgartirilmaganini ko‘rsatish uchun dalil qayerdan va qachon olingani, kimlar unga ishlov bergani, saqlash sharoiti va yaxlitligini tekshirish natijalari hujjatlashtirilishi zarur. Bu talablar aniq protsessual tartib bilan qo‘llab-quvvatlanmasa, dalilning ishonchliligi va maqbulligini baholash murakkablashadi. Budapesht konvensiyasi kiberjinoyatlarni kriminalizatsiya qilish bilan birga, kompyuter ma’lumotlarini tezkor saqlash, qidirish va xalqaro hamkorlikka oid normalarni ham qamrab oladi. O‘zbekiston ushbu konvensiya ishtirokchisi bo‘lmagani sababli uning normalari avtomatik ravishda milliy majburiyat hisoblanmaydi. Shunga qaramay, konvensiyada nazarda tutilgan mexanizmlarni tahlil qilish milliy qonunchilikdagi ehtiyojlarni aniqlashga yordam beradi. Bunda har qanday yangi vakolat inson huquqlari, shaxsiy hayot daxlsizligi, sud nazorati va qonuniylik kafolatlari bilan muvozanatli bo‘lishi kerak.

Qiyosiy tahlil shuni ko‘rsatadiki, AQSh qonunchiligi kompyuter tizimlariga ruxsatsiz kirish va ayrim tegishli xatti-harakatlarga, Buyuk Britaniya qonunchiligi esa



kompyuter tizimidan ruxsatsiz foydalanishga oid jinoyatlarga e'tibor qaratadi. Yevropa Ittifoqining GDPR hujjati shaxsga doir ma'lumotlarni qayta ishlashning qonuniyligi, ma'lumot subyekting huquqlari va ma'lumotlar xavfsizligiga doir talablarni belgilaydi. [8]. Singapurning Cybersecurity Act hujjati muhim kompyuter tizimlari va kiberxavfsizlik bo'yicha vakolatli choralar masalasiga qaratilgan Yaponiya qonunchiligi esa ruxsatsiz kompyuterga kirish va unga bog'liq xatti-harakatlarni tartibga soladi. Bu hujjatlarni O'zbekiston qonunchiligiga to'g'ridan-to'g'ri ko'chirish emas, balki huquqiy yechimlarning maqsadi va kafolatlarini qiyoslash maqsadga muvofiqdir.

Tadqiqot natijasida uchta asosiy muammo ajratildi. Birinchidan, elektron dalillarni aniqlash, olish, saqlash, yaxlitligini tekshirish va sudga taqdim etish bosqichlarida yagona amaliy standartlarga ehtiyoj mavjud. Ikkinchidan, transchegaraviy jinoyatlarda xorijiy vakolatli organlardan ma'lumot olish tezligi va huquqiy tartib-taomillarning muvofiqligi muhim ahamiyatga ega. Uchinchidan, aholining raqamli savodxonligi va tashkilotlarda xavfsizlik madaniyatini rivojlantirish texnik himoya bilan bir qatorda olib borilishi kerak. Maqolaning ilmiy-amaliy yangiligi kiberjinoyatchilikka qarshi kurashish mexanizmlarini besh mezon — jinoiy-huquqiy tartibga solish, infratuzilma xavfsizligi, elektron dalillar, shaxsiy ma'lumotlar himoyasi va xalqaro hamkorlik — asosida birgalikda baholash yondashuvini taklif etsak, ushbu yondashuv alohida qonunlarni mustaqil ko'rib chiqish bilan cheklanmay, ularning o'zaro bog'liqligi va amaliy qo'llanishidagi bo'shliqlarni aniqlashga qaratilgan. Takliflar maqolada o'tkazilgan normativ va qiyosiy tahlildan kelib chiqib, ular empirik tajriba yoki alohida so'rov natijasi sifatida taqdim etilmaydi.

Xulosa. Xulosa qilib aytganda kiberjinoyatchilik bugungi raqamli dunyoning eng dolzarb muammolaridan biridir. Internet va zamonaviy texnologiyalar insonlar hayotini yingillashtirishi bilan birga, turli xil xavf-xatarlarni ham yuzaga keltirmoqda. Kiberjinoyatchilikni oldini olish uchun aholining raqamli savodxonligini oshirish, shaxsiy ma'lumotlarni himoya qilish, kuchli parollardan foydalanish va internetda hushyor bo'lish muhim ahamiyatga ega. Shuningdek, bu borada huquqiy



nazoratni kuchaytirish va yoshlar orasida kiberxavfsizlik madaniyatini shakllantirish zarur. Zero, kiberjinoyatchilikka qarshi kurashish nafaqat huquqni muhofaza qiluvchi organlarning, balki har bir internet foydalanuvchilarining ham mas'uliyatidir. Faqat hamkorlik, bilim va ogohlik orqali xavfsiz raqamli muhitni yaratish mumkin.

Kiberjinoyatchilik raqamli xizmatlardan foydalanish kengaygani sari huquqiy, tashkiliy va texnik jihatdan murakkablashib borayotgan muammolardan biridir. O'zbekiston qonunchiligida kiberxavfsizlik, shaxsga doir ma'lumotlarni himoya qilish va axborot texnologiyalari sohasidagi jinoiy qilmishlarga doir asoslar mavjud. Shu bilan birga, ushbu normalarning samarali ishlashi elektron dalillar bilan ishlash amaliyoti, vakolatli organlar o'rtasidagi muvofiqlashtirish va fuqarolarning raqamli savodxonligiga ham bog'liq.

Budapesht konvensiyasi va xorijiy davlatlar qonunchiligi qiyosiy-huquqiy tahlil uchun foydali manbalardir, biroq O'zbekistonning konvensiyaga a'zoligi va undan kelib chiqadigan majburiyatlar haqidagi fikrlar rasmiy ishtirokchilar ro'yxatiga muvofiq bayon qilinishi kerak. Tadqiqot asosida elektron dalillarni hujjatlashtirish protokolini ishlab chiqish, idoralararo hamkorlikni takomillashtirish, qonuniylik va inson huquqlari kafolatlarini saqlash hamda profilaktika ishlarini kuchaytirish taklif etildi. Mazkur takliflarni amaliyotga joriy etish kiberjinoyatlarni tergov qilish samaradorligini oshirish va raqamli muhitda fuqarolarning huquqlarini himoya qilishga ko'maklashishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasi Konstitutsiyasi. Yangi tahrir. 2023-yil 30-aprel kuni referendumda qabul qilingan.
2. O'zbekiston Respublikasining 2022-yil 15-apreldagi O'RQ-764-son "Kiberxavfsizlik to'g'risida"gi Qonuni.
3. O'zbekiston Respublikasining 2019-yil 2-iyuldagi O'RQ-547-son "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni.
4. O'zbekiston Respublikasining Jinoyat kodeksi. 1994-yil 22-sentabr. Axborot texnologiyalari sohasidagi jinoyatlarga oid XX¹ bob.



5. O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-son “Axborotlashtirish to‘g‘risida”gi Qonuni.

6. Council of Europe. Convention on Cybercrime. Budapest, 23 November 2001. ETS No. 185.

7. O‘zbekiston Respublikasining Ma‘muriy javobgarlik to‘g‘risidagi kodeksi. 1994-yil 22-sentabr.

8. O‘zbekiston Respublikasining 2015-yil 9-dekabrdagi O‘RQ-395-son “Elektron hukumat to‘g‘risida”gi Qonuni.

9. O‘zbekiston Respublikasining 2022-yil 12-oktabrdagi O‘RQ-793-son “Elektron raqamli imzo to‘g‘risida”gi Qonuni.

10. United States. Computer Fraud and Abuse Act. 18 U.S.C. § 1030.

11. United Kingdom. Computer Misuse Act 1990.

12. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation — GDPR). 2016.

13. Singapore. Cybersecurity Act 2018.

14. Japan. Act on Prohibition of Unauthorized Computer Access. Act No. 128 of 1999.

15. O‘zbekiston Respublikasi Hukumat portali. “Kiberjinoyatlarni oldini olishga qaratilgan islohotlar: zamonaviy tahdidlarga qarshi samarali choralar”. 12.03.2026.