Zamonaviy tahdidlar va jinoyat-huquqiy tahlil

(Kiberjinoyatlar)

Berdaq nomidagi davlat universiteti “Yuridika” fakulteti 1-bosqich talabasi

Baltaniyazova Nilufar

https://orcid.org/0009-0004-0055-7949

kuatbaevanilufar65@gmail.com

Annotatsiya: Ushbu maqolada zamanoviy jamiyatimizda kiberjinoyatlar-ning o’rni, xavf darajasi,kelib chiqish sabablari va turlari yanada jinoyat-huquqiy jihatdan tahlili ko’rib chiqiladi.Zamonaviy duyoda axbarot texnologiyalar jadal rivojlanyotgan sharoitda ijtimoiy tamoqlar ya’niy internetda va komputer tizimlarida jinoyatlar oshib yil sayin son sonaqsiz darajaga yetyabti. Xusasan,internetta,ijtimoiy tarmoqlarda va kompyuter tizimlarida firibgarlik,shaxsiy ma’lumotlarni og’irlash, bank tizimiga naqonuniy kirish,viruslarni tarqatish,ijtimoiy tarmoqlarda har xil apk fayllar yuborish orqali akkountlarni og’irlash kabi kiberjinoyatlat jamiyatimizda global muammoga aylanib boryapti.Ilmiy maqqolada kiberjinoyatlarning oldini olish,ularning huquqiy tabiati,aniqlash va javobgarlik masalalari bo’yicha O’zbekiston Respublikasi Jinoyat Kodeksi normalari asosida yoritiladi va axborat xavfsizligini ta’minlash va qonunchilikni takomillashtirish bo’yicha taklif va tavsiyalar ishlab chiqilgan.

Kalit so’zlar: raqamli texnologiyalar, axborat xavfsizligi, Jinoiy javobgarlik, onlayn firibgarliklar, kiberjinoyatlar,

Kirish

Hozirgi davrda jamiyatimizda raqamli texnologiyalar barcha sohalarga chuqurlashib kirib bormaqta,axborat texnologiyalar insonlar hayotining ajralmas hayotiga aylanyapti. Hozirda internet tarmog’i ommalashuv sababidan davlatimiz xam sekin raqamlashtirishka otyabti yanada onlayn bank xizmatlari, sovda-

sotiq,ta’lim,electron to’lovlar va ijtimoiy tarmoqlar odamlar hayotining ajralmas bo’lagiga aylanip bormoqta.Bu halot jamiyat rivojlanishta muhim kasb etadi.Biroq bu jarayon bilan ijtimoiy tarmoqlarda sodir etiliyotgan jinoyatlar soni kun sayin oshib boryapti, yanada yangi turdagi jinoyatlar ochib bormaqta ana shunday jinoyatlar biri kiberjinoyatlar paydo boldi.

Kiberjinoyatlar- bu internet tarmog’i axborat texnologiyalar va raqamli texnologiyalar,kompyuter tizimlari orqali sodir etilyotgan jinoyatlardirBunday jinoyadirtlar orqali firibgarlik,bank kartalaridan pul og’irlash va ma’lumotlarni naqonuniy qo’lga kiritish.Ular davlat,jamiyat va shaxs manfaatlariga jiddiy zarar yetkazishi mumkin.Nafaqat shaxslarga bunday jinoyatlar davlatlar iqtisodiyotiga ham katta zarar keltiradi.Shu bois kiberjinoyatlar nafaqal huquqshunoslar,balki davlat va jamiyatimizning dolzarb masalasi hisoblanadi. Jahon amaliyoti shuni ko’rsatadiki, kiberjinoyatlar an’anaviy jinoyatlarga nisbatan tez tarqaladi va ularni aniqlash ancha murakkab hisoblanadi. Shu sababli kiberxavfsizlik masalasi davlatlar xavfsizligining muhim yo’nalishlaridan biriga aylangan.

Adabiyotlar tahlili va Metadologiyasi

Raqamli texnologiyalar: Kiberjinoyatlar muammosi so’nggi yillarda ko’plab olimlar va mutaxassislar tomonidan keng o’rganilayotgan dolzarb mavzulardan biri hisoblanadi.Raqamli texnologiyalarning jadal rivojlanishi natijasida internet orqali sodir etilyotkan jinoyatlar soni ortib bormoqta.Shu sababli kiberjinoyatlar,axborat xavfsizligi hamda raqamli makondi himoya qilish masalalari ilmiy tadqiqotlarda alohida o’rin tutadi.

Axborat xavfsizligi O’zbekiston Respublikasi hukumati tomonidan ham ushbu muammo ustuvor yo’nalishlardan biri sifatida e’tirof etilgan. Xususan, 2022–2026-yillarga mo’ljallangan Taraqqiyot strategiyasida kiberxavfsizlik strategiyasini ishlab chiqish, axborot xavfsizligini ta’minlash hamda kiberjinoyatlar uchun jinoiy javobgarlikni takomillashtirish bo’yicha muhim vazifalar belgilangan. Bu esa

mamlakatimizda kiberjinoyatchilikka qarshi kurashish bo'yicha huquqiy va tashkiliy mexanizmlarni mustahkamlashga qaratilganligini ko'rsatadi.[3]

Tadqiqot metodologiyasi: Mazkur tadqiqotni amalga oshirish jaroyanida bir qatorda ilmiy uslubiy yondashuvlar va tadqiqot usullaridan foydalaniladi. tadqiqotning metodologik asosini kiberjinoyatchilik,axborot xavfsizligi hamda raqamli texnologiyalar sohasidagi jinoyatlar bilan bog'liq ilmiy adabiyotlar,normative-huquqiy hujjatlar va xalqora tajribalarni o'rganish tashkil etdi. Tadqiqot davomida avvola kiberjinoyatlar tushunchasi, ularning turlari hamda jamiyat uchun keltirib chiqaradigan xavflari ilmiy adabiyotlar asosida tahlil qilindi.Shu bilan birga, O'zvekiston Respublikasining amaldagi qonunchiligi , xususan O'zbekiston Respublikasi Jinoyat Kodeksining XX1 bobi – "Axborat texnologiyalar sohasidagi jinoyatlar"(**278^1–278^9-MODDALAR**) va 168-moddasida mazmunan o'rganilib, ushbu moddalarda nazarda tutilgan jinoiy javobgarlik choralari tahlil qilindi. Shuningdek, tadqiqot jarayonida "Kiberxavfsizlik to'g'risida"gi Qonun, O'zbekiston Respublikasining 2022–2026-yillarga mo'ljallangan Taraqqiyot strategiyasi, shuningdek axborot xavfsizligini ta'minlashga qaratilgan boshqa normativ-huquqiy hujjatlar o'rganildi. Mazkur hujjatlar kiberjinoyatchilikka qarshi kurashish bo'yicha davlat siyosatining asosiy yo'nalishlarini aniqlashga yordam berdi.

Tadqiqot davomida tahlil, qiyosiy-huquqiy tahlil, umumlashtirish va tizimli yondashuv kabi ilmiy usullardan foydalanildi. Qiyosiy-huquqiy tahlil usuli orqali O'zbekiston qonunchiligidagi normalar xalqaro huquqiy hujjatlar bilan solishtirildi. Xususan, Kiberjinoyatchilik to'g'risidagi Budapesht konvensiyasi qoidalari ham o'rganilib, milliy qonunchilikdagi normalar bilan qiyoslandi. Bundan tashqari, tadqiqot davomida statistik ma'lumotlar, ilmiy maqolalar hamda mutaxassislarning fikrlari ham o'rganildi. Bu esa kiberjinoyatchilikning zamonaviy ko'rinishlari va ularning jamiyatga ta'sirini yanada chuqurroq tahlil qilish imkonini berdi.

Natijada, qo'llanilgan metodologik yondashuvlar kiberjinoyatchilikka qarshi kurashish bo'yicha amaldagi huquqiy mexanizmlarni o'rganish, ularning samaradorligini baholash hamda ushbu sohada mavjud muammolarni aniqlashga xizmat qildi.

Tahlil va natijalar:

Onlayn firibgarliklar O'tkazilgan tadqiqotlar shuni ko'rsatadiki, zamonaviy axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda kiberjinoyatlar soni ham ortib bormoqda. Internet tarmoqlari, raqamli xizmatlar va elektron to'lov tizimlaridan keng foydalanish ayrim shaxslar tomonidan noqonuniy maqsadlarda ham qo'llanilmoqda. Natijada kompyuter tizimlariga noqonuniy kirish, shaxsiy ma'lumotlarni o'g'irlash, zararli dasturlar tarqatish hamda turli xil internet firibgarligi kabi jinoyatlar keng tarqalmoqda. Sudlar amaliyotida axborot texnologiyalaridan foydalangan holda sodir etilgan jinoyatlar tobora ko'payib borayotgani kuzatilmoqda. Shu sababli bunday jinoyatlarni to'g'ri kvalifikatsiya qilish hamda ularni boshqa turdagi jinoyatlardan aniq ajratish muhim ahamiyat kasb etadi. O'zbekiston Respublikasi Oliy sudi Plenumi qarorlarida ham axborot texnologiyalari bilan bog'liq jinoyatlarni to'g'ri huquqiy baholash masalalariga alohida e'tibor qaratilgan. Masalan, sud amaliyotida bank va moliya sohasida sodir etiladigan jinoyatlarni axborot texnologiyalari orqali sodir etilgan jinoyatlardan ajratish zarur hisoblanadi. Oliy sud Plenumi tushuntirishlariga ko'ra, jabrlanuvchining bank yoki moliyaviy ma'lumotlarini aldov yo'li bilan qo'lga kiritish O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasi (firibgarlik) bo'yicha baholanadi. Biroq kompyuter tarmoqlariga ruxsatsiz kirish, ma'lumotlarni noqonuniy qo'lga kiritish yoki o'zgartirish bilan bog'liq harakatlar Jinoyat kodeksining 278^2-moddasi asosida javobgarlikka sabab bo'ladi. Shu bois jinoyatlarni to'g'ri kvalifikatsiya qilishda elektron dalillar, texnik ekspertiza, elektron izlar va skrinshotlar muhim ahamiyat kasb etadi. Jinoyat kodeksining 278^1-moddasi kompyuter axborotiga noqonuniy kirish bilan

bog'liq jinoyatlar uchun javobgarlikni nazarda tutadi. Ushbu modda bo'yicha kompyuter tizimlari yoki axborot resurslariga ruxsatsiz kirish holatlari aniqlangan taqdirda aybdor shaxsga jarima, muayyan huquqlardan mahrum qilish yoki boshqa jazo choralarini qo'llash mumkin.[1]

Jinoyat kodeksining 278^4-moddasi kompyuter axborotini modifikatsiyalash, ya'ni ma'lumotlarni o'zgartirish, yo'q qilish yoki ularga zarar yetkazish bilan bog'liq harakatlar uchun jinoiy javobgarlikni belgilaydi. Bunday harakatlar axborot tizimlarining ishlashiga jiddiy zarar yetkazishi hamda davlat yoki tashkilotlarning axborot xavfsizligiga tahdid solishi mumkin. .[1]

Kiberjinoyatlar: Shu bilan birga, amaliyotda ayrim masalalar hali ham qo'shimcha huquqiy tartibga solishni talab etadi. Jumladan, kriptoaktivlar, blokcheyn texnologiyalari va raqamli aktivlar bilan bog'liq huquqbuzarliklarni aniqlash va ularni Jinoyat kodeksining tegishli moddalari bilan kvalifikatsiya qilishda ayrim qiyinchiliklar yuzaga kelmoqda. Bu esa mazkur sohada qonunchilikni yanada takomillashtirish zarurligini ko'rsatadi. Ichki ishlar vazirligi tomonidan e'lon qilingan statistik ma'lumotlarga ko'ra, so'nggi yillarda kiberjinoyatlar soni keskin oshgan. Masalan, 2019-yilda axborot texnologiyalari vositasida sodir etilgan 863 ta jinoyat qayd etilgan bo'lsa, 2024-yilga kelib ularning soni 58,8 ming taga yetgan. Natijada kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 2023-yildagi 6,2 foizdan 2024-yilda 44,4 foizgako'tarilgan. Bu holat kiberjinoyatchilik nafaqat texnologik muammo, balki ijtimoiy xavf tug'diruvchi keng ko'lamli hodisaga aylanganini ko'rsatadi.[2]

Taklif va tavsiyalar

Davlat organlari o'rtasidagi hamkorlikni kuchaytirish muhim: Kiberjinoyatlarga qarshi samarali kurashish uchun Ichki ishlar vazirligi, Markaziy bank, prokuratura organlari hamda boshqa tegishli tashkilotlar o'rtasida axborot almashinuvi va hamkorlik mexanizmlarini rivojlantirish zarur.

Bank va moliya tizimida axborot xavfsizligini mustahkamlash kerak: Banklar va moliya institutlari zamonaviy kiberxavfsizlik tizimlarini joriy etishi, tranzaksiyalar monitoringini kuchaytirishi hamda mijozlarning moliyaviy ma’lumotlarini himoya qilish choralarini kuchaytirishi lozim.

Aholining kiberxavfsizlik bo’yicha bilimini oshirish zarur: Fuqarolar o’rtasida internetdan xavfsiz foydalanish, shaxsiy ma’lumotlarni himoya qilish va kiberfiribgarlikdan ehtiyot bo’lish bo’yicha targ’ibot va tushuntirish ishlarini kengaytirish muhim ahamiyatga ega.

Xalqaro hamkorlikni rivojlantirish muhim: Kiberjinoyatlar ko’pincha xalqaro xarakterga ega bo’lganligi sababli, boshqa davlatlar bilan axborot almashinuvi va hamkorlikni rivojlantirish hamda xalqaro konvensiyalar doirasida tajriba almashish zarur.

Xulosa

Xulosa qilib aytganda, kiberjinoyatlar bugungi kunda zamonaviy jamiyatda tobora dolzarb muammolardan biriga aylanib bormoqda. Axborot texnologiyalarining tez rivojlanishi, internet hamda turli raqamli xizmatlarning keng qo’llanilishi insonlar hayotini ancha yengillashtirdi. Biroq shu bilan birga, internet orqali sodir etilayotgan turli huquqbuzarliklar soni ham ortib bormoqda. Ayniqsa, bank kartalari orqali pul mablag’larini o’g’irlash, internet firibgarligi hamda shaxsiy ma’lumotlarni noqonuniy qo’lga kiritish kabi holatlar jamiyat uchun jiddiy xavf tug’dirmoqda. Kiberjinoyatlarning yana bir muhim jihati shundaki, bunday jinoyatlar ko’pincha yashirin tarzda sodir etiladi va ularni aniqlash an’anaviy jinoyatlarga qaraganda murakkabroq hisoblanadi. Ko’p hollarda jinoyatchilar boshqa davlat hududida turib harakat qilishi ham mumkin. Shu sababli kiberjinoyatlarga qarshi kurashishda nafaqat milliy darajadagi choralar, balki xalqaro hamkorlik ham muhim ahamiyat kasb etadi.

Umuman olganda, kiberjinoyatlarga qarshi samarali kurashish uchun davlat organlari, huquqni muhofaza qiluvchi tashkilotlar va jamiyatning barcha qatlamlari

birgalikda harakat qilishi zarur. Faqat shunda axborot makonida xavfsizlikni ta’minlash va fuqarolar manfaatlarini samarali himoya qilish mumkin bo’ladi.

Foydalangan adabiyotlar:

1. O’zbekiston Respublikasi Jinoyat kodeksi. – T.: Adolat, 2023. https://lex.uz/docs/111453
2. O’zbekiston Respublikasining “Kiberxavfsizlik to’g’risida”gi Qonuni. https://share.google/pyjSEkUtHiI9Qdf6G
3. O’zbekiston Respublikasi 2022–2026-yillarga mo’ljallangan Taraqqiyot strategiyasi. https://lex.uz/docs/5841063
4. O’zbekiston Respublikasi Prezidentining 153-sonli “Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga qarshi kurashni kuchaytirish chora-tadbirlari to’g’risida”gi qaror https://share.google/LUjaKfizw4QTV4p00
5. Convention on Cybercrime (Budapest Convention). Council of Europe, 2001. https://www.coe.int/en/web/cybercrime/the-budapest-convention
6. Kaspersky. Cybersecurity and Cybercrime Report. https://www.kaspersky.com/resource-center
7. O’zbekiston Respublikasi Oliy sudi Plenumining “Firibgarlikka oid ishlar bo’yicha sud amaliyoti to’g’risida”gi qarori. https://share.google/tcPwBTXHr1OmitAQ2
8. Ichki ishlar vazirligi huzuridagi Kiberxavfsizlik markazi statistik tahlillari, 2019–2024-yillar. https://share.google/WHNvbVEcHuAD99dxz
9. Daryo.uz analitik maqolasi: “O’zbekistonda kiberjinoyatlar soni 25 baravar oshdi”, 2024-yil 27-avgust. – daryo.uz