



**INTERNET FIRIBGARLIGI VA KIBERJINOYATLAR: JINOYAT-  
HUQUQIY TAVSIF, HUQUQIY TARTIBGA SOLISH VA QARSHI  
KURASHNING SAMARALI MEXANIZMLARI**

*Donoboyev Ilyosbek Akbar o'g'li.*

*Sarbo'n universiteti "Yurisprudensiya"*

*yo'nalishi 2-kurs talabasi.*

*Ilmiy rahbar: Eshtemirov Komiljon G'ayrat o'g'li.*

*Huquqiy fanlar kofedراسي*

**Annotatsiya:** Mazkur ilmiy maqolada zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi sharoitida keng tarqalib borayotgan internet firibgarligi va kiberjinoyatlarning nazariy-huquqiy asoslari kompleks tarzda tahlil qilinadi. Tadqiqot doirasida internet firibgarligining jinoyat-huquqiy mohiyati, uning jinoyat tarkibi elementlari (obyekt, obyektiv tomon, subyekt va subyektiv tomon) chuqur yoritilib, ushbu jinoyat turining an'anaviy firibgarlikdan farqli jihatlari asoslab beriladi. Xususan, internet firibgarligining anonimlik, transmilliylik, tezkorlik va ommaviylik kabi xususiyatlari uning ijtimoiy xavflilik darajasini sezilarli darajada oshirishi ilmiy jihatdan izohlanadi. Maqolada internet firibgarligining zamonaviy ko'rinishlari, jumladan phishing, vishing, smishing, elektron to'lov tizimlari orqali firibgarlik, ijtimoiy tarmoqlardagi scam sxemalari, kriptovalyuta bilan bog'liq firibgarlik hamda sun'iy intellekt texnologiyalaridan foydalanilgan yangi avlod jinoyat usullari tizimli ravishda tasniflanadi va ularning har biri jinoyat-huquqiy nuqtayi nazardan baholanadi. Shu bilan birga, ushbu jinoyatlarni sodir etishda qo'llaniladigan ijtimoiy muhandislik usullari va psixologik ta'sir mexanizmlarining o'rni ham alohida ko'rib chiqiladi. Tadqiqotda O'zbekiston Respublikasining amaldagi normativ-huquqiy bazasi, xususan Jinoyat kodeksining 168-moddasi (firibgarlik), 278-moddasi (kompyuter axborotiga ruxsatsiz kirish) hamda "Axborotlashtirish to'g'risida" va "To'lovlar va to'lov tizimlari to'g'risida"gi qonunlar asosida internet firibgarligi uchun javobgarlik masalalari



tahlil qilinadi. Amaliyotda uchrayotgan asosiy muammolar, jumladan jinoyatni kvalifikatsiya qilishdagi murakkabliklar, dalillarni to'plash va mustahkamlashdagi qiyinchiliklar, kiber ekspertiza zarurati hamda jinoyatchilarni aniqlashdagi transmilliy to'siqlar ilmiy asosda yoritiladi. Shuningdek, maqolada kiberjinoyatlarning kriminologik xususiyatlari, ularning yuzaga kelish sabablari va sharoitlari, jinoyatchilarning tipologiyasi hamda jabrlanuvchilar doirasi tahlil qilinadi. Internet firibgarligining oldini olishda profilaktika choralari, jumladan aholining huquqiy va raqamli savodxonligini oshirish, axborot xavfsizligi madaniyatini shakllantirish, zamonaviy texnologik himoya vositalarini joriy etish hamda huquqni muhofaza qiluvchi organlarning institutsional salohiyatini mustahkamlash zarurligi asoslab beriladi. Bundan tashqari, tadqiqotda kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlikning ahamiyati ochib berilib, davlatlar o'rtasida axborot almashinuvi, qo'shma tergov amaliyoti va global xavfsizlik mexanizmlarini rivojlantirishning dolzarbligi ta'kidlanadi. Yakuniy xulosalar sifatida internet firibgarligiga qarshi kurashish samaradorligini oshirish uchun huquqiy, texnologik, institutsional va ijtimoiy yo'nalishlarni o'z ichiga olgan kompleks yondashuv zarurligi ilmiy asosda ilgari suriladi.

**Kalit so'zlar:** internet firibgarligi, kiberjinoyat, kriminologiya, phishing, ijtimoiy muhandislik, axborot xavfsizligi, elektron to'lov tizimlari, huquqiy javobgarlik, transmilliy jinoyatlar.

Zamonaviy jamiyatda raqamli texnologiyalar rivoji inson faoliyatining deyarli barcha sohalarini qamrab oldi. Internet orqali amalga oshirilayotgan iqtisodiy operatsiyalar, elektron davlat xizmatlari, bank tizimlari va ijtimoiy tarmoqlar keng qo'llanilmoqda. Shu bilan birga, ushbu jarayonlar jinoyatchilikning yangi shakllari, xususan kiberjinoyatlarning paydo bo'lishiga olib keldi. Internet firibgarligi bugungi kunda eng keng tarqalgan va ijtimoiy xavfli jinoyatlardan biri hisoblanadi. Uning asosiy xususiyatlari quyidagilardan iborat: yuqori darajadagi yashirinlik; tezkor amalga oshirish; keng auditoriyani qamrab olish imkoniyati; transmilliy xarakter. O'zbekiston Respublikasida ushbu soha quyidagi normativ-huquqiy hujjatlar bilan tartibga solinadi: Jinoyat kodeksi (168-modda — firibgarlik, 278-



modda — kompyuter axborotiga ruxsatsiz kirish); “Axborotlashtirish to‘g‘risida”gi Qonun; “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonun; Axborot xavfsizligi va kiberxavfsizlik sohasidagi davlat siyosati hujjatlari.

Mazkur maqolaning ilmiy yangiligi shundaki, unda internet firibgarligi nafaqat jinoyat-huquqiy, balki kriminologik, texnologik va institutsional jihatdan ham kompleks o‘rganiladi. Internet firibgarligining nazariy-huquqiy mohiyati shundaki Internet firibgarligi — bu jinoyat huquqida firibgarlikning zamonaviy ko‘rinishi bo‘lib, unda axborot texnologiyalari asosiy vosita sifatida qo‘llaniladi.

Jinoyat kodeksining 168-moddasiga ko‘ra: Firibgarlik — bu o‘zganing mulkini yoki mulkiy huquqini aldov yoki ishonchni suiiste‘mol qilish yo‘li bilan qo‘lga kiritishdir.

Internet firibgarligi ushbu moddaning quyidagi elementlari asosida baholanadi:

Obyekt: mulkiy munosabatlar; iqtisodiy xavfsizlik. Obyektiv tomon: aldov (fake sayt, soxta akkaunt); ishonchni suiiste‘mol qilish (bank xodimi sifatida chiqish); zarar yetkazish. Subyekt: umumiy subyekt (16 yoshdan); ko‘pincha IT bilimga ega shaxslar. Subyektiv tomon: to‘g‘ridan-to‘g‘ri qasd; moddiy manfaat olish niyati.

Internet firibgarligining kengaytirilgan kriminologik tahlili. Internet firibgarligi an‘anaviy jinoyatlardan quyidagi jihatlar bilan farq qiladi:

Yashirinlik: Jinoyatchilar VPN, anonim akkauntlar orqali faoliyat yuritadi.

Transmilliylik: Jinoyat bir davlatdan turib boshqa davlat fuqarosiga nisbatan sodir etiladi.

Ommaviylik: Bir vaqtning o‘zida minglab foydalanuvchilar nishonga olinadi.

Psixologik ta‘siri - jinoyatchilar qo‘rqitish (kartangiz bloklanadi), shoshiltirish (tez tasdiqlang), ishonch uyg‘otish usullaridan foydalanadi.

Internet firibgarligining chuqurlashtirilgan tasnifi:

-Phishing. Huquqiy baho: JK 168, JK 278.

-Vishing. Telefon orqali aldash — firibgarlik sifatida baholanadi.



-Smishing. SMS orqali fishing — ham jinoyat tarkibiga kiradi.

-BEC (Business Email Compromise). Kompaniya nomidan pul o'tkazishga majbur qilish.

- Carding. Bank kartalari ma'lumotlarini o'g'irlash.

- Kripto firibgarlik. Regulyatsiya yetarli emasligi sababli murakkab.

- Deepfake firibgarligi. Sun'iy intellekt yordamida aldash — yangi xavf turi.

Jinoyatni kvalifikatsiya qilishdagi murakkabliklar: Amaliyotda bir nechta modda qo'llanadi, jinoyat tarkibi chalkash bo'ladi, zarar miqdorini aniqlash qiyin, normativ bazada maxsus "kiberfiribgarlik" tushunchasi yo'q, Dalillarni yig'ish va isbotlash muammolari.

Kiberjinoyatlarda asosiy dalillar: IP loglar; tranzaksiya tarixi; elektron yozishmalar. Muammolar shundaki serverlar chet davlatdaligi, ma'lumotlar tez o'chin ketishi, ekspertiza murakkabligi, jinoyatchini aniqlash qiyin, dalillar yetarli emasligi, texnik bilim yetishmasligi; sudlarda kiber masalalar bo'yicha tajriba kam.

Xalqaro huquqiy mexanizmlarda Kiberjinoyatlar global muammo bo'lib: davlatlar o'rtasida hamkorlik zarur, ekstraditsiya va ma'lumot almashinuvi muhim. Masalan Interpol va boshqa tashkilotlar jinoyatchilarni aniqlashda yordam beradi. Internet firibgarligiga qarshi kurashning kompleks modeli shundaki alohida kiberjinoyat normasi kiritish, jazoni kuchaytirish, texnologik yechimlar ya'ni antifraud tizimlar, AI monitoring, biometrik himoya. Ta'lim va profilaktikaga oid yechimlar: aholining huquqiy savodxonligini oshirish, yoshlar bilan ishlash. Kiberpolitsiya, maxsus ekspertlar tayyorlashga doir chora tadbirlarni oshirish.

Ilmiy taklif va tavsiyalar

1. Jinoyat kodeksiga "kiberfiribgarlik" tushunchasini kiritish
2. Kiberjinoyatlar bo'yicha alohida bob yaratish
3. Sud va tergov organlarini texnik jihatdan kuchaytirish
4. Bank tizimida xavfsizlik standartlarini oshirish
5. Xalqaro hamkorlikni kengaytirish

**Xulosa.** Internet firibgarligi zamonaviy raqamli jamiyat sharoitida nafaqat alohida shaxslar mulkiy manfaatlariga, balki butun iqtisodiy tizim va davlat



axborot xavfsizligiga real tahdid soluvchi murakkab va ko‘p qirrali jinoyat turi hisoblanadi. Ushbu jinoyatlarning asosiy xususiyati ularning yuqori darajadagi yashirinligi, tezkorligi, transmilliy xarakterga egaligi hamda zamonaviy axborot texnologiyalariga tayangan holda amalga oshirilishidir. Amaldagi huquqiy tartibga solish tizimi, xususan O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi orqali firibgarlik jinoyatlariga umumiy huquqiy baho berilayotgan bo‘lsa-da, internet muhitida sodir etiladigan jinoyatlarning o‘ziga xos xususiyatlari ularni kvalifikatsiya qilish, dalillarni to‘plash va jinoyatchilarni aniqlash jarayonida bir qator murakkabliklarni yuzaga keltirmoqda. Ayniqsa, kompyuter axborotiga noqonuniy kirish, elektron to‘lov tizimlaridan foydalanish va shaxsiy ma’lumotlarni qo‘lga kiritish bilan bog‘liq holatlar ko‘pincha bir nechta jinoyat tarkibining uyg‘unlashuvi sifatida namoyon bo‘lib, huquqni qo‘llash amaliyotida aniq yondashuvni talab etadi. Shu bilan birga, kiberjinoyatlarning tez sur‘atlarda rivojlanib borayotgani, yangi usullar — phishing, vishing, smishing, kriptoalyuta va sun‘iy intellekt asosidagi firibgarlik shakllarining paydo bo‘lishi amaldagi qonunchilikni doimiy ravishda takomillashtirib borishni taqozo etadi. Amaliyotda yuzaga kelayotgan muammolar, xususan jinoyatchilarning anonimligi, xorijiy serverlardan foydalanilishi, dalillarni tez yo‘qolishi va texnik ekspertiza zarurati kiberjinoyatlarga qarshi kurashishda faqat an’anaviy yondashuvlar yetarli emasligini ko‘rsatadi. Shu sababli, ushbu sohada zamonaviy texnologik vositalarni keng joriy etish, kiberxavfsizlik tizimlarini mustahkamlash, bank va moliyaviy institutlar faoliyatida yuqori darajadagi himoya mexanizmlarini qo‘llash muhim ahamiyat kasb etadi. Bundan tashqari, internet firibgarligiga qarshi samarali kurashishda profilaktika choralari alohida o‘rin tutadi. Aholining huquqiy va raqamli savodxonligini oshirish, fuqarolarda axborot xavfsizligi madaniyatini shakllantirish, ijtimoiy tarmoqlar va ommaviy axborot vositalari orqali ogohlantirish ishlarini kuchaytirish jinoyatlarning oldini olishda muhim vosita hisoblanadi. Shu bilan birga, huquqni muhofaza qiluvchi organlarning kiberjinoyatlar bo‘yicha malakasini oshirish, maxsus bo‘linmalar faoliyatini rivojlantirish hamda kiber ekspertiza tizimini takomillashtirish zarur. Internet firibgarligining transmilliy xususiyatini inobatga olgan holda, xalqaro hamkorlikni



kengaytirish, xorijiy davlatlar bilan tezkor axborot almashinuvi va qo‘shma tergov mexanizmlarini yo‘lga qo‘yish ham dolzarb masalalardan biri hisoblanadi. Umuman olganda, internet firibgarligiga qarshi kurashish samaradorligi faqatgina jazolash choralariga emas, balki huquqiy, texnologik, institutsional va ijtimoiy omillarni o‘z ichiga olgan kompleks yondashuvga bog‘liq bo‘lib, aynan shu yo‘l bilan ushbu xavfli jinoyat turining oldini olish va uning salbiy oqibatlarini minimallashtirish mumkin.

### FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasi Jinoyat kodeksi
2. “Axborotlashtirish to‘g‘risida”gi Qonun
3. “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonun
4. Kiberxavfsizlik bo‘yicha davlat dasturlari
5. Interpol materiallari
6. UNODC hisobotlari
7. Jinoyat huquqi