# KIBERJINOYATLARNI FOSH ETISHDA TARMOQ IPLARINING O‘RNI VA JINOYAT-PROTSESSUAL VA KRIMINALISTIK AHAMIYATI

*IIV Akademiyasi Raqamli texnologiyalar*
*va axborot xavfsizligi kafedrasi boshlig‘i,*
*fizika matematika fanlari nomzodi*
*dotsent* ***A.A.Iminov***
*IIV Akademiyasi kunduzgi ta’lim*
*3-bosqich 315-guruh kursanti safdor*
***Rashidov Sharof Mansur o‘g‘li***

**Annotatsiya**

Ushbu ilmiy maqolada zamonaviy kiberjinoyatlarni fosh etishda raqamli izlar, xususan, tarmoq paketlari, log-fayllar va IP-manzillar (tarmoq iplari)ning o‘rni hamda kriminalistik ahamiyati tadqiq qilingan. Virtual makonda sodir etilayotgan transmilliy xarakterdagi kiber-tahdidlarni aniqlashda global tarmoq provayderlarining ma'lumotlar bazasi va server jurnallaridan foydalanishning yuridik mexanizmlari tahlil etilgan. Maqolada raqamli dalillarni jinoyat protsessida qonuniy rasmiylashtirish (legallashtirish) muammolari ko‘rib chiqilib, Jinoyat-protsessual kodeksiga raqamli tarmoq ma'lumotlarini klassifikatsiya qilishga qaratilgan normalarni kiritish bo‘yicha amaliy va ilmiy takliflar ilgari surilgan.

**Kalit so‘zlar:** *kiberjinoyat, raqamli izlar, IP-manzil, log-fayl, tarmoq trafigi, kriminalistika, dalillarni legallashtirish, kiber-fosh etish, provayder.*

## Kirish

Global axborotlashuv va raqamli texnologiyalar asrida jamiyat hayotining barcha jabhalari internet makoniga integratsiya qilinmoqda. Raqamli platformalar, elektron to‘lov tizimlari va virtual muloqot tarmoqlari insonlar mushkulini oson qilish bilan bir qatorda, jinoiy guruhlar uchun ham yangicha huquqbuzarlik vositasi bo‘lib xizmat qilmoqda. Kiberjinoyatchilik (kiber-firsummary, bank kartalaridan mablag‘larni qonunsiz o‘zlashtirish, fishing va kiber-terrorizm) o‘zining anonimligi, transchegaraviyligi va yashirinligi bilan an'anaviy jinoyatchilik turlaridan tubdan farq qiladi.

Kiber-makonda an'anaviy ma'nodagi qon, barmoq izi yoki moddiy ashyolar qolmaydi; u yerda faqatgina elektron yoki raqamli izlar mavjud bo‘ladi. Kiberjinoyatchini aniqlash va jinoiy qilmishni fosh etishda eng asosiy bog‘lovchi bo‘g‘in — bu virtual dunyodan jismoniy dunyoga olib chiquvchi "tarmoq iplari" (IP-manzillar, routing jurnallari, MAC-manzillar va log-fayllar) hisoblanadi. Shu sababli, tarmoq izlarini to‘g‘ri identifikatsiya qilish, ularni kriptografik saqlash va jinoyat

protsessida dalil sifatida qonuniy legallashtirish masalalarini tadqiq etish kiber-xavfsizlik va huquqni muhofaza qilish organlari oldidagi eng dolzarb vazifadir.

**1. Kiber-makonda raqamli izlar va tarmoq iplarining kriminalistik tavsifi**

Kriminalistika fanining fundamental qoidalariga ko‘ra, har qanday harakat tashqi muhitda o‘z aksini qoldiradi. Kiberjinoyat sodir etilganda ham tarmoq arxitekturasida muayyan izlar zanjiri hosil bo‘ladi. Axborot texnologiyalari terminologiyasidagi ushbu izlar majmuasini yuridik tilda "tarmoq iplari" deb atash mumkin. Ushbu iplarning eng birinchi elementi IP (Internet Protocol) manzildir. IP-manzil global tarmoqqa ulangan har bir qurilmaga beriladigan unikal raqamli identifikator bo‘lib, u jinoyat sodir etilgan virtual nuqtani geografik va fizik hudud bilan bog‘lash imkonini beradi.

Biroq, zamonaviy kiberjinoyatchilar ko‘pincha o‘zlarining haqiqiy tarmoq manzillarini yashirish maqsadida proksi-serverlar, VPN (Virtual Private Network) tizimlari va Tor brauzerlari (Darknet) kabi anonimlashtiruvchi vositalardan foydalanadilar. Bunday murakkab sharoitda faqatgina oxirgi IP-manzilni bilish yetarli emas. Kriminalist va kiber-ekspertlar tarmoq provayderlarining serverlaridagi log-fayllarni (kirish-chiqish jurnallarini), DNS so‘rovlarini va paketli ma'lumotlar oqimini tahlil qilish orqali zanjirsimon "tarmoq iplarini" bir-biriga bog‘lab, haqiqiy kiberjinoyatchining lokatsiyasini aniqlash taktikalaridan foydalanadilar.

**2. Tarmoq ma'lumotlaridan kiberjinoyatlarni fosh etishda foydalanish mexanizmlari**

Tarmoq iplari va raqamli izlarni to‘plash asosan tezkor-qidiruv tadbirlari hamda tergov harakatlari davomida amalga oshiriladi. Mazkur jarayon uchun huquqni muhofaza qiluvchi organlar va telekommunikatsiya provayderlari (aloqa operatorlari) o‘rtasidagi tezkor va tizimli hamkorlik talab etiladi. Provayderlar qonunchilikka muvofiq foydalanuvchilarning tarmoq faolligi to‘g‘risidagi ma'lumotlarni muayyan muddat davomida saqlashga majburdirlar.

Kiber-firsummary yoki xakerlik hujumi sodir bo‘lganda, tergovchi sud sanktsiyasi yoki qonuniy so‘rov asosida provayderlardan jinoyat sodir etilgan vaqtdagi tarmoq ulanishlari jurnallarini talab qilib oladi. Ushbu jurnallar yordamida jinoyatchining qaysi aloqa operatori orqali, qaysi baza stansiyasi (geografik hudud) doirasida va qaysi unikal qurilma (IMEI yoki MAC-manzil) yordamida tarmoqqa kirgani aniqlanadi. Mazkur elektron izlar jinoyatni sodir etgan shaxsni to‘g‘ridan-to‘g‘ri ayblashga emas, balki uni jismoniy dunyoda qidirib topish va uning qurilmalarida (kompyuter, smartfon) ashyoviy dalillarni to‘plash uchun poydevor yaratadi.

**3. Tarmoq izlarini jinoyat protsessida dalil sifatida legallashtirish muammolari**

Tezkor usullar bilan olingan tarmoq iplarini jinoyat ishi hujjatlariga qonuniy dalil sifatida kiritish eng ziddiyatli huquqiy jarayondir. Muammo shundaki, raqamli

ma'lumotlar o‘ta o‘zgaruvchan (volatile) bo‘lib, ularni osongina o‘chirish, o‘zgartirish yoki soxtalashtirish mumkin. Agar tergovchi yoki tezkor xodim provayderdan olingan log-faylni yoki IP-manzil aks etgan elektron hujjatni prosessual normalarga rioya etmagan holda rasmiylashtirsa, sud uni nomaqbul dalil deb topishi mumkin.

Amaldagi Jinoyat-protsessual kodeksida "tarmoq trafigi", "log-fayllar" yoki "raqamli tarmoq izlari" tushunchalarining aniq prosessual tasnifi mavjud emas. Ko‘pincha bunday ma'lumotlar oddiy "hujjatlar" yoki "ashyoviy dalillar" sifatida ishga qo‘shiladi, bu esa himoya tarafiga (advokatlarga) raqamli dalillarning haqiqiyligini shubha ostiga qo‘yish uchun huquqiy zamin yaratadi. Shuningdek, xorijiy serverlar (masalan, chet eldagi VPN provayderlari) orqali sodir etilgan jinoyatlarda xalqaro huquqiy hamkorlikning sustligi "tarmoq iplari"ning uzilishiga olib kelmoqda.

**Tadqiqot natijalari va takliflar**

Kiberjinoyatlarni fosh etishda tarmoq izlari va iplaridan foydalanish samaradorligini oshirish maqsadida quyidagi tashkiliy-huquqiy va ilmiy takliflar ilgari suriladi:

1. JPKga yangi protsessual tushunchalarni kiritish: Jinoyat-protsessual qonunchiligiga "tarmoq izi", "virtual identifikator" va "provayder log-fayli" kabi tushunchalarni va ularni dalil sifatida qabul qilishning o‘ziga xos mezonlarini qonuniy muhrlash.

2. "Raqamli ashyoviy dalillarni ta'minlash" institutini joriy etish: Kiberjinoyat izlari o‘chib ketishining oldini olish uchun tergovchiga sud sanktsiyasisiz, lekin keyinchalik sudni xabardor qilish sharti bilan tarmoq ma'lumotlarini provayderlarda 48 soatgacha muzlatib qo‘yish (fast-freeze) vakolatini berish.

3. SMT (Sud-media va kiber-ekspertiza) markazlarini rivojlantirish: Tarmoq trafigi va log-fayllar ustida tezkor sud-kriminalistik ekspertizalarini o‘tkazish tartibini soddalashtirish va ushbu yo‘nalishda kadrlar malakasini oshirish.

**Xulosa**

Xulosa qilib aytganda, virtual makondagi har qanday jinoiy qilmish ortidan raqamli izlar zanjirini qoldiradi. Tarmoq iplari (IP-manzillar, log-fayllar) kiberjinoyatchining shaxsini va uning jinoiy qilmishlarini fosh etishda markaziy o‘rinni egallaydi. Kiber-makonda qonun ustuvorligi va jinoiy javobgarlikning muqarrarligini ta'minlash ushbu raqamli izlarni to‘g‘ri aniqlash va ulardan jinoiy protsessda samarali foydalanish mexanizmlarining mukammalligiga bevosita bog‘liqdir.

**Foydalanilgan adabiyotlar ro‘yxati**

1. O‘zbekiston Respublikasining Konstitutsiyasi. – Toshkent: “O‘zbekiston”, 2023 y.
2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. O‘RQ-764-son, 2022 yil 15 aprel.
3. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi. – Toshkent: “Adolat”,

2025 y.
4. Rassulov A.X. Kiberjinoyatchilik kriminalistikasi: Darslik. – Toshkent: IIV Akademiyasi, 2023. – 290 b.
5. Karimov M.A. Raqamli dalillar bilan ishlashning prosessual xususiyatlari // Huquqiy tadqiqotlar jurnali. – 2024. – №4. – B. 45-52.
6. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
7. Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.