

**INTERNET TARMOG'IDA SODIR ETILGAN FIRIBGARLIK  
JINOYATLARINI TERGOV QILISH SAMARADORLIGINI OSHIRISH  
ISTIQBOLLARI**

**Xabibiddinov Nodirjon Mo'sinjon o'g'li**

Toshkent davlat yuridik universiteti mustaqil izlanuvchisi,

Sud hokimiyati, advokatura va huquqni muhofaza

qiluvchi organlar sho'basini o'qituvchisi

ORCID: 0009-0009-5402-2364

E-mail: [nodirjonxabibiddinov@gmail.com](mailto:nodirjonxabibiddinov@gmail.com)

***Annotatsiya.** Ushbu tezisda internet tarmog'ida sodir etilgan firibgarlik jinoyatlarini tergov qilish samaradorligini oshirish istiqbollari ilmiy-amaliy nuqtayi nazardan tahlil qilingan. Raqamlashtirish sharoitida internet firibgarligining keskin o'sib borayotganini statistik ma'lumotlar asosida asoslanib, ushbu toifadagi jinoyatlarni tergov qilishda yuzaga keladigan obyektiv qiyinchiliklar: anonimlik, transchegaraviylik va raqamli dalillarning tez yo'qoluvchanligi ko'rsatib o'tilgan. Tadqiqotda maxsus bilimlardan foydalanish, xususan kompyuter-texnik ekspertizasi hamda raqamli dalillarni to'plashning xalqaro standartlari tergov samaradorligini oshirishdagi hal qiluvchi roli ochib berilgan. Qiyosiy-huquqiy tahlil orqali AQSh, Yevropa Ittifoqi va boshqa davlatlar tajribasi o'rganilib, milliy qonunchilik va tergov amaliyotini takomillashtirishga qaratilgan aniq takliflar ishlab chiqilgan.*

**Kalit soʻzlar:** *internet firibgarligi, kiberjinoyatchilik, maxsus bilimlar, raqamli (elektron) dalillar, kompyuter-texnik ekspertizasi, kriminalistika*

**Abstract.** This thesis analyzes the prospects for increasing the efficiency of investigating fraudulent crimes committed on the Internet from a scientific and practical perspective. Based on statistical data regarding the sharp increase in internet fraud in the context of digitalization, objective difficulties arising in the investigation of this category of crimes are shown: anonymity, cross-border nature, and the rapid disappearance of digital evidence. The study reveals the decisive role of using specialized knowledge, specifically computer-technical expertise and international standards for collecting digital evidence, in increasing the effectiveness of investigations. Through comparative legal analysis, the experience of the USA, the European Union, and other countries was studied, and specific proposals aimed at improving national legislation and investigative practice were developed.

**Keywords:** internet fraud, cybercrime, specialized knowledge, digital (electronic) evidence, computer-technical expertise, criminalistics.

Oxirgi yillarda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va jamiyat hayotining barcha jabhalari raqamlashuvi internet tarmogʻidan foydalangan holda sodir etiladigan jinoyatlar koʻlamining keskin kengayishiga sabab boʻldi. Ularning eng keng tarqalgan va ijtimoiy xavfli

turlaridan biri internet firibgarligi hisoblanadi. Bunday jinoyatlar moddiy zarar yetkazish bilan birga, fuqarolarning raqamli xizmatlarga bo'lgan ishonchiga ham putur yetkazadi.

Muammoning miqyosi xalqaro statistikada yaqqol namoyon bo'ladi. AQSh Federal tergov byurosining Internet jinoyatlari bo'yicha shikoyatlar markazi ma'lumotlariga ko'ra, 2024-yilda 859 532 ta shikoyat qayd etilib, yetkazilgan zarar 16,6 milliard AQSh dollaridan oshgan; bu ko'rsatkich bir yil ichida 33 foizga ko'paygan. Umumiy zararining qariyb 83 foizi aynan firibgarlik turidagi jinoyatlarga to'g'ri keladi, investitsion firibgarlik bo'yicha zarar esa 6,5 milliard dollardan ortgan [1].

O'zbekistonda kiberxavfsizlikni ta'minlash 2025-yil yakuniga kelib yana-da kun tartibining muhim masalasiga aylandi. Ichki ishlar vazirligi hamda Kiberxavfsizlik markazining ma'lumotlari shuni ko'rsatadiki, mamlakatda kiberjinoyatlar miqdori so'nggi besh yil mobaynida 68 barobarga ko'paygan - agar 2019-yilda 863 ta holat qayd etilgan bo'lsa, 2024-yilga kelib bu raqam 58 800 taga yetgan. Natijada fuqarolar ko'rgan umumiy zarar 1,9 trillion so'mdan oshgan bo'lib, uning 98 foizi aynan bank kartalari orqali amalga oshirilgan firibgarliklar ulushiga to'g'ri keladi [2]. Davlat tomonidan ko'rilayotgan choralar, jumladan O'zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi "Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida"gi PQ-153-sonli qaroriga muvofiq, kiberjinoyatlar yo'nalishida tergov faoliyati samaradorligini

o'shinish hamda ta'lim jarayonini takomillashtirishni ilmiy va uslubiy jihatdan ta'minlash chora-tadbirlari belgilandi [3]. Shunga qaramay, ushbu jinoyatlarni tergov qilish amaliyoti hanuzgacha jiddiy qiyinchiliklarga duch kelmoqda. Bu esa internet firibgarligini tergov qilish samaradorligini o'shinish masalasini dolzarb ilmiy muammo darajasiga ko'taradi.

Internet firibgarligi an'anaviy mulkka qarshi jinoyatlardan o'zining bir qator o'ziga xos kriminalistik xususiyatlari bilan ajralib turadi va aynan shu jihatlar tergov jarayonini sezilarli darajada murakkablashtiradi. Avvalo, bunday jinoyatlarga yuksak darajadagi anonimlik xosdir: jinoyatchilar VPN-xizmatlar, anonimlashtiruvchi tarmoqlar, soxta akkauntlar va kriptovalyuta hamyonlaridan foydalangan holda o'z shaxsini yashiradi, bu esa aybdorni aniqlash va uning aybdorligini isbotlashni qiyinlashtiradi. Ikkinchidan, internet firibgarligi ko'pincha transchegaraviy tabiatga ega bo'lib, jinoyatchi bir davlatda, jabrlanuvchi ikkinchi davlatda, jinoyat sodir etilgan server esa uchinchi davlatda joylashishi mumkin; bunday sharoitda samarali tergov xalqaro huquqiy yordam va tezkor hamkorlik mexanizmlariga tayanishni taqozo etadi. Uchinchidan, raqamli dalillarning o'zgaruvchanligi va tez yo'qoluvchanligi alohida muammo sifatida namoyon bo'ladi, zero elektron izlar oson o'zgartirilishi yoki butunlay yo'q qilinishi mumkin, shu bois ularni o'z vaqtida hamda metodik jihatdan to'g'ri qo'lga olish hal qiluvchi ahamiyat kasb etadi. To'rtinchidan, ma'lumotlarning shifflanishi va kriptovalyutalar orqali mablag' o'tkazish jinoiy yo'l bilan olingan daromadlarning izini yo'qotib, ularni kuzatishni murakkablashtiradi. Nihoyat, tergovchilarning maxsus tayyorgarligi yetishmasligi ham jiddiy to'siq bo'lib qolmoqda: raqamli dalillar bilan ishlash chuqur texnik bilimni talab qiladi va bunday salohiyatning

yeterli emasligi qo'lg'a olingan dalillarning protsessual ahamiyatini yo'qotishiga olib kelishi mumkin.

Sanab o'tilgan omillar internet firibgarligini tergov qilishda an'anaviy uslublarning yetarli emasligini va maxsus bilimlardan tizimli foydalanish zaruratini ko'rsatadi.

Shuningdek, jinoyatlarni tergov qilishda maxsus bilimlardan foydalanish ham muhim rol o'ynaydi. Maxsus bilimlar deganda fan, texnika, san'at va hunar sohasiga oid, umumiy foydalanishda bo'lmagan hamda huquqni qo'llash faoliyatida mutaxassis yoxud ekspert ishtirokida tatbiq etiladigan ixtisoslashgan bilimlar majmui tushuniladi. Internet firibgarligini tergov qilish jarayonida bunday bilimlar hal qiluvchi, hatto markaziy ahamiyat kasb etadi, zero ushbu toifadagi jinoiy ishlar bo'yicha shakllantiriladigan dalillar bazasining asosiy qismi texnik mohiyatga ega bo'lib, ularni to'g'ri idrok etish, baholash va talqin qilish maxsus tayyorgarlikni taqozo etadi. Shu nuqtayi nazardan, mutaxassisning tergov harakatlarida, ayniqsa birlamchi bosqich - voqea joyini ko'zdan kechirish, tintuv o'tkazish va elektron qurilmalarni qo'lg'a olish jarayonida ishtirok etishi raqamli izlarning yo'qolishi yoki buzilishi xavfini sezilarli darajada kamaytiradi va dalillarning protsessual ahamiyatini saqlab qolishga xizmat qiladi. Bunda qo'lg'a olingan ma'lumotlarning yaxlitligi va asl holatini ta'minlash maqsadida xesh-summalarni hisoblash, yozuvni bloklovchi texnik vositalardan foydalanish, shuningdek dalillarning qo'lg'a olingan paytdan sud jarayonigacha bo'lgan uzluksiz nazorat zanjirini izchil hujjatlashtirish kabi metodik talablarga qat'iy rioya etilishi zarur.

Kompyuter-texnik ekspertizasi esa o'chirilgan ma'lumotlarni tiklash, tranzaksiyalar va tarmoq jurnallarini tahlil qilish, foydalanuvchilarni identifikatsiyalash hamda jinoiy mablag'lar harakatini kuzatish imkonini beradi. Bunday ekspertizaning metodik jihatdan to'g'ri o'tkazilishi raqamli dalillarni to'plash bo'yicha xalqaro standartlarga, xususan ISO/IEC 27037:2012 standartiga (raqamli dalillarni aniqlash, yig'ish, qo'lga olish va saqlash bo'yicha qo'llanma) tayanishni taqozo etadi[4]. Aynan shu standartlarga rioya etilishi raqamli dalilning sud jarayonida yo'l qo'ysa bo'ladigan (huquqiy kuchga ega) dalil sifatida e'tirof etilishini ta'minlaydi.

Rivojlangan davlatlar tajribasi internet firibgarligiga qarshi kurashda tashkiliy, huquqiy va texnik choralarning uyg'unligi muhimligini ko'rsatadi. AQShda shikoyatlarni markazlashgan tarzda qabul qilish va tahlil qilish, shuningdek noqonuniy o'tkazilgan mablag'larni tezkor "muzlatish" mexanizmi orqali jabrlanuvchilarga yordam ko'rsatadi. Bunday markaz idoralararo va xalqaro hamkorlikni muvofiqlashtirish uchun ham xizmat qiladi.

Yevropa Ittifoqida Yevropa kiberjinoyatchilikka qarshi markazi a'zo davlatlar o'rtasida operativ ma'lumot almashinuvini ta'minlaydi. Xalqaro huquqiy asos sifatida 2001-yilda qabul qilingan kiberjinoyatchilik to'g'risidagi Budapesht konvensiyasi alohida ahamiyatga ega: u elektron dalillarni tezkor saqlash, 24/7 rejimida ishlovchi aloqa nuqtalari va transchegaraviy hamkorlikning protsessual asoslarini belgilab beradi [5]. Raqamli dalillar bilan ishlash sohasida ISO/IEC 27037, 27041, 27042 va 27043 standartlari xalqaro me'yoriy negiz vazifasini bajaradi.

Ushbu tajriba O'zbekiston uchun ham muhim ahamiyatga ega bo'lib, milliy tizimni xalqaro standartlar va hamkorlik mexanizmlariga muvofiqlashtirish tergov samaradorligini sezilarli darajada oshirishi mumkin.

O'tkazilgan tahlil natijalari internet firibgarligini tergov qilish samaradorligini oshirish kompleks yondashuvni taqozo etishini ko'rsatadi, bunda har bir taklif aniq amalga oshirish mexanizmi bilan ta'minlangan bo'lishi lozim.

Birinchi navbatda, O'zbekiston Respublikasi Jinoyat-protsessual kodeksini raqamli (elektron) dalillarni qo'lga olish, saqlash, tadqiq etish va ularning yaxlitligini ta'minlash protsessual tartibini aniq belgilovchi normalar bilan to'ldirish maqsadga muvofiq. Buning mexanizmi sifatida kodeksga elektron dalilning tushunchasi va turlarini mustahkamlovchi, shuningdek uni qo'lga olishda majburiy xesh-summa hisoblash, holatni bayonnomada aks ettirish va guvohlar yoki videoyozuv orqali tasdiqlash talablarini nazarda tutuvchi alohida modda (yoki boblar majmui) kiritilishi mumkin.

Ikkinchidan, ISO/IEC 27037 xalqaro standarti asosida raqamli dalillar bilan ishlashning milliy standartini ishlab chiqish va qabul qilish zarur. Bu jarayonni amalga oshirish uchun Adliya vazirligi, Ichki ishlar vazirligi, Sud ekspertizasi markazi ishtirokida idoralararo ishchi guruh tuzilib, standart loyihasi tayyorlanishi hamda u barcha tergov va ekspertlik organlari uchun majburiy texnik reglament sifatida tasdiqlanishi maqsadga muvofiq.

Uchinchidan, kiberjinoyatchilik to'g'risidagi Budapesht konvensiyasiga qo'shilish masalasini ko'rib chiqish lozim, zero bu xalqaro huquqiy yordam va elektron dalillarni tezkor saqlash imkoniyatlarini sezilarli darajada kengaytiradi.

Mexanizm sifatida konvensiya matnini milliy qonunchilikka muvofiqligi yuzasidan ekspertiza qilish, uning 24/7 rejimida ishlovchi aloqa nuqtasi talablariga javob beruvchi vakolatli organi belgilash va qo'shilish to'g'risidagi taklifni belgilangan tartibda kiritish nazarda tutiladi.

To'rtinchidan, tergovchilar va sud ekspertlari uchun raqamli kriminalistika bo'yicha maxsus malaka oshirish dasturlarini joriy etish hamda ixtisoslashgan tergov bo'linmalarini kuchaytirish talab etiladi. Buni amalda ta'minlash uchun oliy ta'lim muassasalari va malaka oshirish markazlari o'quv rejasiga raqamli kriminalistika moduli kiritilishi, amaliy treninglar tashkil etilishi hamda kiberjinoyslarni tergov qiluvchi ixtisoslashgan bo'linmalar shtati va texnik salohiyati mustahkamlanishi mumkin.

Beshinchidan, banklar, to'lov tizimlari va internet-provayderlar bilan tezkor ma'lumot almashinuvi hamda jinoiy mablag'larni tezkor "muzlatish" mexanizmini yo'lga qo'yish zarur. Buning mexanizmi sifatida huquqni muhofaza qiluvchi organlar va moliya institutlari o'rtasida ishlovchi yagona raqamli platforma yaratilishi, unda so'rovlarga belgilangan qisqa muddatda javob berish va shubhali tranzaksiyalarni vaqtincha bloklash tartibi normativ jihatdan mustahkamlanishi mumkin.

Nihoyat, oltinchidan, sud-ekspertlik muassasalarining moddiy-texnik bazasini zamonaviy raqamli kriminalistika dasturiy va apparat vositalari bilan ta'minlash lozim. Bu maqsadda davlat byudjeti yoki maqsadli loyihalar doirasida ekspertlik laboratoriyalarini litsenziyalangan dasturiy vositalar, yozuvni bloklovchi

qurilmalar va ma'lumotlarni tiklash uskunalari bilan jihozlash, shuningdek ularni davriy yangilab borish tizimini yo'lga qo'yish maqsadga muvofiq.

Internet firibgarligini tergov qilish samaradorligi, eng avvalo, maxsus bilimlardan o'z vaqtida va metodik jihatdan to'g'ri foydalanishga bog'liqdir. Raqamli dalillar bilan ishlashning protsessual va texnik standartlarini takomillashtirish, sud ekspertizasi imkoniyatlarini kengaytirish, kadrlar tayyorgarligini kuchaytirish hamda xalqaro hamkorlikni rivojlantirish bu sohada ijobiy natijaga erishishning kalitidir. Taklif etilgan chora-tadbirlarning amaliyotga joriy etilishi internet firibgarligini tergov qilish samaradorligini oshirish, jinoyatlarning oldini olish va fuqarolarning huquq hamda qonuniy manfaatlarini ishonchli himoya qilishga xizmat qiladi.

## **FOYDALANILGAN MANBALAR RO'YXATI**

1. Federal Bureau of Investigation. 2024 Internet Crime Report. - Internet Crime Complaint Center (IC3), 2025. <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>

2. O'zbekiston Respublikasi Ichki ishlar vazirligi Kiberxavfsizlik markazi rasmiy hisobotlari (2019–2025 yillar). Kiberjinoyatlar statistikasi va dinamikasi bo'yicha ma'lumotlar. Manba: <https://iiv.uz> va markazning ochiq hisobotlari. <https://www.gazeta.uz/uz/2025/11/05/cybercrime>

3. 2025-yil 30-apreldagi "Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida"gi PQ-153-sonli qarori. <https://lex.uz/uz/docs/-7511145>

