“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=362

2026-yil
4-son
aprel
ISSN 3093-8546



Internet tarmogʻida sodir etilgan firibgarlik jinoyatlarining kriminalistik tavsifi

Nodirjon Xabibiddinov,
Toshkent davlat yuridik universiteti Sud hokimiyati, advokatura va huquqni muhofaza qiluvchi organlar shoʻbasi oʻqituvchisi
Huquqshunos
e-mail: nodirjonxabibiddinov@gmail.com

Аннотация. Maqolada internet tarmogʻida sodir etiladigan firibgarlik jinoyatlarining kriminalistik tavsifi elementlari tadqiq etilgan. Tadqiqotning dolzarbligi kiberjinoyatchilik koʻlamining global va milliy miqyosda keskin ortishi bilan asoslanadi. Qiyosiy-huquqiy va statistik tahlil metodlari qoʻllanib, jinoyatning sodir etilish mexanizmi uch bosqichda - tayyorgarlik, amalga oshirish va yashirish jarayonlari sifatida tizimlashtirilib, raqamli izlar tizimi, jinoyatchi va jabrlanuvchi shaxsining tipologik xususiyatlari aniqlangan. AQSh, Yevropa Ittifoqi, Buyuk Britaniya va Rossiya tajribasi Oʻzbekiston amaliyoti bilan qiyosiy tahlil qilingan. Natijada internet firibgarligini alohida jinoyat tarkibi sifatida qonunchilikda mustahkamlash, raqamli dalillar bilan ishlashning yagona milliy standartlarini ishlab chiqish va tergov organlari kadrlarining raqamli kriminalistika sohasidagi malakasini oshirish boʻyicha takliflar ilgari surilgan.

Калит сўзлар. kiberjinoyatchilik, internet firibgarligi, kriminalistik tavsif, raqamli izlar, jinoyat mexanizmi, fishing, tergov metodikasi, jinoyatchi portreti.

Аннотация. В статье исследуются элементы криминалистической характеристики мошенничества, совершаемого в сети Интернет. Актуальность исследования обусловлена резким ростом масштабов киберпреступности на глобальном и национальном уровнях. С применением методов сравнительно-правового и статистического анализа механизм совершения преступления систематизирован в виде трёх этапов - подготовки, совершения и сокрытия; также определены система цифровых следов и типологические особенности личности преступника и потерпевшего. Проведён сравнительный анализ опыта США, Европейского союза, Великобритании и России с практикой Узбекистана. В результате были выдвинуты предложения по закреплению интернет-мошенничества в законодательстве в качестве самостоятельного состава преступления, разработке единых национальных стандартов работы с цифровыми доказательствами и повышению квалификации сотрудников следственных органов в области цифровой криминалистики.

Ключевые слова. киберпреступность, интернет-мошенничество, криминалистическая характеристика, цифровые следы, механизм преступления, фишинг, методика расследования, портрет преступника.

Annotation. The article explores the forensic characteristics of fraud committed on the internet. The relevance of the research is underscored by the sharp increase in the scale of cybercrime at both global and national levels. Using comparative-legal and statistical analysis methods, the mechanism of the crime is systematized into three stages: preparation, perpetration, and concealment. The study also identifies the system of digital traces and the typological characteristics of the offender and the victim. A comparative analysis was conducted, contrasting the experiences of the USA, the European Union, Great Britain, and Russia with the practices in Uzbekistan. As a result, proposals have been put forward to codify internet fraud as a distinct criminal offense in legislation, to develop unified national standards for working with digital evidence, and to enhance the skills of investigative personnel in the field of digital forensics.

Keywords. cybercrime, internet fraud, forensic description, digital traces, crime mechanism, phishing, investigative methodology, criminal portrait.

Zamonaviy axborot texnologiyalarining jadal rivojlanishi va internet tarmogʻining kundalik hayotga chuqur kirib borishi natijasida kiberjinoyatchilik muammosi dunyo miqyosida dolzarb muaamoga aylangan. Bugungi kunda kiberjinoyatchilik nafaqat alohida shaxslar va tashkilotlarga, balki butun davlatlarning iqtisodiy barqarorligiga jiddiy tahdid solmoqda. Cybersecurity Ventures tahlillariga koʻra, 2025-yilga kelib kiberjinoyatchilik natijasida dunyo boʻylab yetkaziladigan zarar yillik 10,5 trillion AQSh dollariga yetishi prognoz qilingan boʻlib, bu koʻrsatkich kiberjinoyatchilikni AQSh va Xitoydan keyin dunyodagi uchinchi yirik iqtisodga aylantiradi [1]. Statista Market Insights ma'lumotlariga koʻra, kiberjinoyatchilik natijasida yetkazilgan global zarar 2024-yilda 9,22 trillion dollarni tashkil etgan boʻlib, 2028-yilga kelib 13,82 trillion dollarga yetishi kutilmoqda [2].

Internet firibgarligi kiberjinoyatchilik tarkibida eng keng tarqalgan jinoyat turlaridan biri sifatida ajralib turadi. AQSh Federal qidiruv byurosining (FBI) Internet jinoyatlari shikoyatlari markazi (IC3) 2024-yilgi hisobotiga koʻra, markaz 859 532 ta shikoyat qabul qilgan boʻlib, jabrlanuvchilarning umumiy zarari 16,6 milliard dollardan oshgan — bu koʻrsatkich 2023-yilga nisbatan 33 foizga oʻsganligini anglatadi [3]. Fishing va spoofing 193 407 ta shikoyat bilan eng koʻp qayd etilgan jinoyat turi boʻlgan, investitsion firibgarlik esa 6,57 milliard dollar zarar bilan moliyaviy jihatdan eng ogʻir jinoyat sifatida aniqlangan [4].

Yevropa miqyosida ham vaziyat jiddiy tus olmoqda. Europol tomonidan 2024-yilda nashr etilgan Internet Organised Crime Threat Assessment (IOCTA) hisobotiga koʻra, fishing Yevropa

Ittifoqida firibgarlik sodir etishning eng keng tarqalgan usuli bo‘lib qolmoqda, bunda fuqarolar, xususiy kompaniyalar va davlat muassasalari nishonga olinmoqda. SMS orqali fishing (smishing) eng ko‘p uchraydigan tur sifatida aniqlangan bo‘lsa, QR-kod orqali fishing (quishing) yangi tahdid sifatida paydo bo‘lmoqda [5].

O‘zbekiston Respublikasida internet firibgarligi muammosi o‘ta keskin tus olgan. O‘zbekiston Respublikasi Ichki ishlar vazirligi Kiberxavfsizlik markazi ma'lumotlariga ko‘ra, 2019-yilda axborot texnologiyalari yordamida 18 ta toifadagi 863 ta jinoyat sodir etilgan bo‘lsa, 2024-yilda bu ko‘rsatkich 62 ta toifadagi 58 800 ta jinoyatga yetgan — ya'ni besh yil ichida kiberjinoyatlar soni 68 barobarga o‘sgan [6]. 2021-2024-yillar oralig‘ida kiberjinoyatlar natijasida fuqarolardan 1 trillion 909 milliard so‘mdan ortiq mablag‘ o‘g‘irlangan bo‘lib, faqat 2024-yilning o‘zida zarar 603 milliard so‘mni tashkil etgan. 2024-yilda mamlakatda jami 58 800 ta kiberjinoyat qayd etilgan bo‘lib, ularning 97,7 foizi fuqarolarning bank karta mablag‘lariga noqonuniy kirish bilan bog‘liq [7].

Yuqoridagi statistik ma'lumotlar internet firibgarligi jinoyatlarining kriminalistik tavsifini o‘rganish zaruratini taqozo etadi. Jinoyatlarning sodir etilish usullari, izlar tizimi, jinoyatchi va jabrlanuvchi shaxsining xususiyatlari haqidagi bilimlar tergov amaliyotini takomillashtirish, jinoyatlarni samarali fosh etish va oldini olish uchun muhim ahamiyat kasb etadi. Biroq, mazkur sohadagi ilmiy tadqiqotlar, ayniqsa O‘zbekiston milliy qonunchiligi kontekstida, hali yetarli darajada olib borilmagan.

Internet firibgarligi jinoyatlari o‘zining murakkabligi, ko‘p qirraliligi va doimiy o‘zgarib borishi bilan an'anaviy firibgarlikdan tubdan farq qiladi. Jinoyatchi va jabrlanuvchi bir-birini ko‘rmaydi, turli davlatlarda joylashishi mumkin, jinoyat izlari esa raqamli muhitda saqlanadi va osongina o‘zgartirilishi yoki yo‘q qilinishi mumkin. Shu boisdan, mazkur jinoyatlarni samarali tergov qilish uchun ularning kriminalistik tavsifi elementlarini ilmiy jihatdan chuqur o‘rganish zaruriyati mavjud.

Tadqiqotning asosiy maqsadi internet tarmog‘ida sodir etiladigan firibgarlik jinoyatlarining kriminalistik tavsifi elementlarini aniqlash, ularni tizimlashtirish hamda tergov faoliyatini takomillashtirish bo‘yicha ilmiy asoslangan takliflar ishlab chiqishdan iborat.

Internet firibgarligi jinoyatlarining kriminalistik tavsifiga oid masalalar xorijiy va mahalliy olimlar tomonidan tadqiq etilgan. Kiberjinoyatchilik sohasida Wall tomonidan internet jinoyatlarining klassifikatsiyasi taklif etilgan. Holt va Bossler kiberjinoyatchilik va raqamli kriminalistika bo‘yicha keng qamrovli tadqiqot olib borgan. Casey elektron dalillar va kompyuter kriminalistikasi sohasida muhim ilmiy hissa qo‘shgan.

O‘zbekistonlik olimlardan M.Kh. Rustambayev, G.A. Axmedov, A.Sh. Baratov, B.Xamidov, B.Karimov, O.Ganiyev, R.Abdullayev, D.Bazarova, G.Axmedova va boshqalar jinoyat huquqi va kriminalistika sohasida muhim tadqiqotlar olib borgan. Shu bilan

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

birga, internet firibgarligi jinoyatlarining kriminalistik tavsifiga bag‘ishlangan maxsus tadqiqotlar kam bo‘lib, bu borada chuqur ilmiy tadqiqotlar olib borish zarurati mavjud.

Internet firibgarligi jinoyatlarining kriminalistik tavsifini o‘rganish bir vaqtning o‘zida huquqiy, texnik, psixologik va ijtimoiy jihatlarni qamrab oladigan jarayon bo‘lib, bu holat bir necha ilmiy metodning uyg‘unlashgan holda qo‘llanilishini taqozo etadi.

Maqolada qiyosiy-huquqiy metod orqali O‘zbekiston Respublikasining internet firibgarligiga qarshi qonunchiligi AQSh, Rossiya Federatsiyasi, Buyuk Britaniya va Yevropa Ittifoqi davlatlarining tegishli normativ-huquqiy bazasi bilan solishtirma tahlil qilindi, bu esa milliy qonunchilikdagi bo‘shliqlarni aniqlash imkonini berdi. Statistik tahlil metodi O‘zbekiston Respublikasi Ichki ishlar vazirligi, xalqaro tashkilotlar hisobotlaridagi raqamli ko‘rsatkichlarni qayta ishlash, jinoyatlarning dinamikasi va tarkibiy taqsimotini aniqlash imkonini berdi. Shu bilan birga, internet firibgarligi sohasida latent jinoyatchilik darajasi yuqori bo‘lib, rasmiy statistika faqat qayd etilgan holatlarni aks ettirishini hisobga olish lozim.

Maqolada internet firibgarligining kriminalistik tavsifiga doir muallif ta‘rifi bir qator xorijiy va mahalliy ilmiy manbalar tahlili asosida, xususan, Jensen va boshq. (2021), Broadhurst va boshq. (2019), Europol (2022) hisobotlari o‘rganildi va quyidagicha shakllantirildi:

Internet firibgarligi — bu axborot-kommunikatsiya texnologiyalari va internet tarmog‘idan foydalangan holda boshqa shaxslarning mol-mulkini yoki pul mablag‘larini noqonuniy ravishda egallashga qaratilgan qasddan sodir etiladigan ijtimoiy xavfli xatti-harakatdir.

An’anaviy firibgarlikdan farqli o‘laroq, internet firibgarligida jinoyatchi jabrlanuvchi bilan bevosita aloqa o‘rnatmaydi, balki texnik vositalar va raqamli kommunikatsiya kanallari orqali aldov yoki ishonchni suiste’mol qilish harakatini amalga oshiradi. Aynan shu xususiyat mazkur jinoyat turiga kriminalistik nuqtayi nazardan alohida yondashish zarurligini belgilaydi.

O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi firibgarlikni — ya'ni boshqa shaxsning mol-mulkini egallash yoki mol-mulkka bo‘lgan huquqni qo‘lga kiritishni aldov yoki ishonchni suiste‘mol qilish yo‘li bilan sodir etilgan holda javobgarlikni belgilaydi. Shu bilan birga, Jinoyat kodeksining XX1 -bobi axborot texnologiyalari sohasidagi jinoyatlar uchun alohida javobgarlikni nazarda tutadi. Biroq, amaliyotda internet firibgarligini kvalifikatsiya qilishda muayyan qiyinchiliklar mavjud — jinoyatning bir vaqtning o‘zida ham aldov elementi, ham axborot texnologiyalaridan noqonuniy foydalanish belgisini o‘z ichiga olganligi sababli, tergov organlari ko‘pincha moddalar tanlashda ikkilanishga duch keladi. Bu holat internet firibgarligining mustaqil jinoyat tarkibi sifatida qonunchilikda belgilanishi masalasini kun tartibiga qo‘yadi.

Internet firibgarligining quyidagi asosiy turlari mavjud:

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Birinchidan, fishing (phishing) hujumlari internet firibgarligining eng keng tarqalgan va eng koʻp zarar yetkazadigan turlaridan biridir. Bu usulda jinoyatchilar banklar, davlat organlari yoki mashhur xizmat koʻrsatish platformalari nomidan soxta elektron xatlar, SMS-xabarlar yoki veb-saytlar yaratib, foydalanuvchilarning login, parol, bank karta raqamlari va CVV-kodlari kabi maxfiy ma'lumotlarini qoʻlga kiritadi.

Oʻzbekistonda fishing hujumlari asosan Telegram messenger va SMS orqali amalga oshirilmoqda. Jinoyatchilar bank xodimlari yoki davlat organlari vakillari sifatida oʻzlarini tanishtiradi va jabrlanuvchilardan SMS-kod talab qiladi. Gazeta.uz maʻlumotlariga koʻra, yil boshidan buyon messenjerlar va ijtimoiy tarmoqlarda 1200 ga yaqin firibgarlik reklama kampaniyalari aniqlangan boʻlib, ularning aksariyati mashhur xizmatlar sahifalarini nusxalaydigan fishing saytlari koʻrinishida tashkil etilgan.

Ikkinchidan, soxta onlayn-doʻkonlar va e-tijorat firibgarligi tobora kengayib bormoqda. Bu turda jinoyatchilar professional koʻrinishdagi veb-saytlar yaratib, bozor narxidan ancha past narxlarda tovarlar taklif etadi, oldindan toʻlov talab qiladi, soʻngra tovarni yetkazib bermaydi yoki sifatsiz mahsulot joʻnatadi. Kriminalistik nuqtayi nazardan, bu jinoyatlarning oʻziga xos jihati shundaki, jinoyatchilar qisqa muddatda koʻplab jabrlanuvchilardan nisbatan kichik miqdordagi mablagʻlarni yigʻadi, bu esa har bir alohida holatda jabrlanuvchini huquqni muhofaza qilish organlariga murojaat qilishdan toʻsadi. Oʻzbekiston IIV Kiberxavfsizlik markazi ma'lumotlariga koʻra, onlayn savdo platformalaridagi firibgarlik barcha kiberjinoyatlarning 11 foizini tashkil etadi [8]. Amaliyot shuni koʻrsatadiki, soxta onlayn-doʻkonlar koʻpincha bayram va chegirma mavsumlarida faollashadi, bu esa jabrlanuvchilarning past narxga boʻlgan ishonchidan foydalanish strategiyasini koʻrsatadi. Bunday jinoyatlarni tergov qilishda domen registratsiyasi ma'lumotlari, xosting provayderlar bilan hamkorlik va toʻlov tizimlarining tranzaksiya tarixi muhim dalil manbai boʻlib xizmat qiladi.

Uchinchidan, jinoyatchilar Facebook, Instagram, Telegram va boshqa platformalarda soxta profillar yaratib, uzoq vaqt davomida jabrlanuvchining ishonchini qozonadi va keyin turli bahonalar bilan pul mablagʻlarini soʻraydi. Bu turga romantik firibgarlik (romance scam), soxta xayriya yigʻimlari, soxta lotereyalar va piramidal sxemalar kiradi. FBI IC3 hisobotiga koʻra, moliyaviy “grooming” firibgarliklari — ya'ni jabrlanuvchi bilan uzoq muddatli ishonchli munosabat oʻrnatib, keyin mablagʻlarni tortib olish usuli — 2024-yilda kriptovalyuta orqali 2,5 milliard dollardan ortiq mablagʻ jalb qilgan [9].

Oʻzbekistonda ijtimoiy tarmoqlardagi firibgarlikning oʻziga xos shakli — bu “Salom, onam” (Hello, Mom) sxemasi boʻlib, bunda jinoyatchi jabrlanuvchining yaqin qarindoshi sifatida murojaat qiladi va shoshilinch pul oʻtkazishni talab qiladi. Kriminalistik jihatdan bu jinoyatlarni tergov qilishda asosiy qiyinchilik

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

jinoyatchilarning bir nechta soxta profillardan foydalanishi, virtual telefon raqamlarini qoʻllashi va olingan mablagʻlarni koʻplab hisobvaraqlar orqali tezda tarqatib yuborishidir.

Toʻrtinchidan, kriptovalyuta va investitsion firibgarlik oxirgi yillarda eng tez oʻsayotgan va eng koʻp moliyaviy zarar yetkazayotgan jinoyat turiga aylanmoqda. Jinoyatchilar yuqori foyda va'da qilib, jabrlanuvchilarni soxta investitsion platformalarga jalb etadi, dastlab kichik foydalar koʻrsatib ishonch hosil qiladi, soʻngra yirik mablagʻ kiritilgandan keyin platforma yopiladi va mablagʻlar oʻgʻirlanadi. Bu usul xalqaro amaliyotda “pig butchering” (choʻchqa boqish) deb nomlanadi — jinoyatchi jabrlanuvchini “semirtiradi”, keyin barcha mablagʻini tortib oladi [10].

Oʻzbekistonda ham kriptovalyuta firibgarligi holatlari koʻpaymoqda. Ayniqsa Telegram kanallari orqali “kafolatlangan daromad” va'da qiladigan soxta investitsion guruhlar faoliyati kengaygan. Biroq, mazkur jinoyatlarni tergov qilishda kriptovalyuta tranzaksiyalarining yarim anonim xarakteri va blokcheyn texnologiyasining murakkabligi jiddiy toʻsiq boʻlib qolmoqda.

Yuqorida koʻrsatilgan toʻrt asosiy turdan tashqari, amaliyotda boshqa shakllar ham kuzatiladi: biznes elektron pochta firibgarligi (BEC) — bunda jinoyatchi kompaniya rahbariyati yoki hamkor tashkilot nomidan soxta xat yuborib, yirik mablagʻ oʻtkazishni talab qiladi; texnik yordam firibgarligi — kompyuterda virus borligi haqida soxta ogohlantirish yuborib, “tuzatish” uchun pul undirish; hamda identifikatsiya oʻgʻirlash — boshqa shaxsning shaxsiy ma'lumotlaridan foydalanib kredit olish yoki moliyaviy operatsiyalar amalga oshirish.

Shuni alohida ta'kidlash lozimki, internet firibgarligining barcha turlari oʻzaro bogʻliq holda qoʻllaniladi. Masalan, fishing hujumi orqali olingan ma'lumotlar investitsion firibgarlikda ishlatilishi yoki ijtimoiy tarmoqdagi soxta profil e-tijorat firibgarligi uchun vosita sifatida xizmat qilishi mumkin. Bu holat kriminalistik tavsif tuzishda jinoyatning alohida turlarini emas, balki butun mexanizmni yaxlit tizim sifatida koʻrib chiqish zarurligini koʻrsatadi. Shuningdek, sun'iy intellekt texnologiyalarining rivojlanishi bilan firibgarlik usullari yanada murakkablashmoqda. Masalan, deepfake videolar, sun'iy ovoz generatsiyasi va AI yordamida yozilgan ishonchli matnlar jinoyatchilarning arsenalini kengaytirmoqda, bu esa kriminalistika fani oldiga yangi vazifalar qoʻymoqda.

Internet firibgarligi jinoyatlarining kriminalistik tavsifida jinoyat sodir etilish mexanizmi markaziy oʻrinni egallaydi, chunki aynan mexanizmni bilish tergov versiyalarini ilgari surish, dalillar bazasini shakllantirish va jinoyatchini aniqlash jarayonining asosini tashkil etadi. An'anaviy firibgarlikda jinoyatchi jabrlanuvchi bilan yuzma-yuz muloqot qilsa, internet firibgarligida bu jarayon butunlay virtual muhitda kechadi — jinoyatchi oʻzini yashirish, soxta shaxsiyat yaratish va geografik chegaralardan qat'iy nazar jinoyatni sodir etish imkoniyatiga ega boʻladi. Bu xususiyat mazkur jinoyatlarning mexanizmini an'anaviy firibgarlikdan sifat jihatidan

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

farqlaydi va kriminalistik tahlilga yangicha yondashishni talab qiladi.

Tadqiqot natijalariga koʻra, internet firibgarligi jinoyatlarining sodir etilish jarayoni uchta asosiy bosqichdan iborat boʻlib, har bir bosqich oʻziga xos kriminalistik ahamiyatga ega izlarni shakllantiradi.

Tayyorgarlik bosqichida jinoyatchi jinoyatni rejalashtiradi va texnik infratuzilmani tayyorlaydi. Bu jarayonda maqsadli auditoriya tanlanadi, soxta veb-sayt, elektron pochta manzili yoki ijtimoiy tarmoq profili yaratiladi, VPN xizmatlari, proksi-serverlar va anonim toʻlov tizimlari sozlanadi. Koʻpgina hollarda jinoyatchi boshqa davlatlar hududida joylashgan serverlardan foydalanadi, bu esa keyinchalik yurisdiksiya masalalarini keltirib chiqaradi. Tayyorgarlik bosqichi kriminalistik jihatdan juda muhim, chunki aynan shu davrda jinoyatchi eng koʻp raqamli iz qoldiradi — domen registratsiyasi maʼlumotlari, xosting xizmati bilan tuzilgan shartnoma, VPN provayderiga toʻlov qaydlari, soxta saytning yaratilish metadata maʼlumotlari kabi izlar keyinchalik jinoyatchini aniqlashda hal qiluvchi dalil boʻlib xizmat qilishi mumkin. Oʻzbekistonda kiberjinoyatchilarning eng koʻp qoʻllaydigan usuli — zararli havolalar va dasturlar orqali bank kartasi yoki mobil qurilma ustidan nazorat oʻrnatish boʻlib, bu usul barcha kiberjinoyatlarning 60 foizini tashkil etadi [11]. Bu maʼlumot tayyorgarlik bosqichida zararli dasturiy taʼminotni tayyorlash va tarqatish kanallarini tashkil etish jinoyatchilarning asosiy faoliyatiga aylanganligini tasdiqlaydi.

Amalga oshirish bosqichida jinoyatchi jabrlanuvchi bilan bevosita aloqa oʻrnatadi va aldov mexanizmini ishga tushiradi. Bu bosqichning davomiyligi jinoyat turiga qarab sezilarli darajada farqlanadi — fishing hujumlarida jarayon bir necha daqiqa ichida yakunlansa, investitsion firibgarlik yoki romantik firibgarlikda jinoyatchi jabrlanuvchining ishonchini bir necha hafta, hatto bir necha oy davomida asta-sekin qozonadi. Europol IOCTA 2024 hisobotida taʼkidlanganidek, sunʼiy intellekt vositalari va deepfake texnologiyalari jinoyatchilarning ijtimoiy muhandislik qobiliyatlarini keskin kuchaytirmoqda, bu esa aldov jarayonini yanada ishonchliroq va aniqlashni qiyinroq qilmoqda [12]. Amalga oshirish bosqichida shakllanadigan izlar orasida elektron yozishmalar mazmuni, telefon qoʻngʻiroqlari qaydlari, jabrlanuvchi hisobvaragʻidan mablagʻ oʻtkazilgan vaqt va yoʻnalishi, shuningdek, jinoyatchi tomonidan foydalanilgan IP-manzillar va qurilma identifikatorlari alohida ahamiyat kasb etadi.

Yashirish bosqichi internet firibgarligi jinoyatlarining eng murakkab va tergov uchun eng qiyin qismidir. Bu bosqichda jinoyatchi olingan mablagʻlarni bir necha bank hisobvaraqlari orqali ketma-ket oʻtkazish, kriptovalyutaga aylantirish yoki uchinchi shaxslar — xalqaro amaliyotda “money mules” deb ataladigan vositachilar orqali naqd pulga aylantirish yoʻllaridan foydalanadi. FBI IC3 va TRM Labs maʼlumotlariga koʻra, 2024-yilda jinoyatchilar firibgarlik mablagʻlarini oʻtkazishda kriptovalyuta, ayniqsa USDT va

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

DAI kabi stablecoinlardan, shuningdek, markazlashmagan moliya (DeFi) platformalaridan keng foydalangan. O‘zbekiston amaliyotida esa mablag‘larni yashirish ko‘proq bir necha bank kartalaridan ketma-ket o‘tkazish va uchinchi shaxslar hisobvaraqlari orqali naqd pul chiqarish usullari bilan amalga oshirilmoqda, biroq kriptovalyutaga o‘tish tendensiyasi ham kuzatilmoqda.

Internet firibgarligi jinoyatlarida qoldirilgan izlar tizimi an'anaviy jinoyatlardan tubdan farq qiladi va kriminalistik fanida “raqamli izlar” (digital traces) tushunchasi bilan ifodalanadi. Raqamli izlar tarkibiga IP-manzillar va geolokatsiya ma'lumotlari, brauzer tarixi va cookie fayllar, elektron yozishmalar va messenjer xabarlari, bank tranzaksiyalari va to‘lov tizimlari qaydlari, server loglari va fayl metadata ma'lumotlari, ijtimoiy tarmoqlardagi faoliyat izlari kiradi. Mazkur izlarning an'anaviy moddiy izlardan asosiy farqi ularning nomoddiy, oson o‘zgartiriladigan va tez yo‘q qilinadigan tabiatidadir — jinoyatchi bir necha daqiqa ichida loglarni o‘chirib tashlashi, IP-manzilni o‘zgartirishi yoki soxta hisobvaraqni yopishi mumkin. Shu boisdan raqamli izlarni o‘z vaqtida fiksatsiya qilish, ularning yaxlitligini ta'minlash va protsessual jihatdan to‘g‘ri rasmiylashtiirsh tergov muvaffaqiyatining hal qiluvchi sharti hisoblanadi.

Shu o‘rinda muhim muammoni qayd etish zarur: O‘zbekistonda raqamli dalillarni yig‘ish va saqlash bo‘yicha yagona metodologik ko‘rsatma hali ishlab chiqilmagan. Amaliyotda tergov organlari xodimlari raqamli izlarni fiksatsiya qilishda turli yondashuvlardan foydalanmoqda, bu esa dalillarning sud tomonidan rad etilishi xavfini oshiradi. Xalqaro amaliyotda esa bu soha ancha rivojlangan. Masalan, AQShda National Institute of Standards and Technology (NIST) tomonidan raqamli kriminalistikaning yagona standartlari ishlab chiqilgan (NIST Special Publication 800-86), Yevropa Ittifoqida esa ENISA raqamli dalillar bilan ishlash bo‘yicha ko‘rsatmalar nashr etgan. O‘zbekiston uchun ham shunga o‘xshash milliy standartlarni ishlab chiqish dolzarb masala bo‘lib qolmoqda.

Kriminalistik tavsifning muhim elementlaridan biri jinoyatchi shaxsining xususiyatlarini aniqlashdir, chunki jinoyatchining demografik, intellektual va psixologik portretini bilish operativ-qidiruv faoliyatini to‘g‘ri yo‘naltirish, qidiruv doirasini toraytirish va tergov versiyalarini asoslash uchun bevosita amaliy ahamiyatga ega.

Tadqiqot doirasida tahlil qilingan materiallar va xalqaro tadqiqotlar natijalari internet firibgarligini sodir etuvchi shaxslarning muayyan tipologiyasini shakllantirish imkonini berdi. Yosh tarkibi jihatidan, internet firibgarlarining asosiy qismi — taxminan 65 foizi — 20 yoshdan 35 yoshgacha bo‘lgan yosh shaxslardir. Bu holat tasodifiy emas: aynan shu yosh guruhi raqamli texnologiyalar bilan o‘sgan, internet muhitini yaxshi tushunadigan va yangi texnik vositalarni tez o‘zlashtiradigan avlodni tashkil etadi. Jinsi bo‘yicha esa 78 foiz holatda jinoyat erkaklar tomonidan sodir etilgan bo‘lib, bu tendensiya nafaqat O‘zbekiston, balki global

miqyosda ham kuzatiladi. Ta'lim darajasiga kelsak, jinoyatchilarning 70 foizdan ortig‘i oliy yoki o‘rta maxsus ta'limga ega bo‘lib, ularning aksariyati axborot texnologiyalari, dasturlash yoki moliya sohasida muayyan bilim va ko‘nikmalarga ega shaxslar hisoblanadi. Bu ma'lumotlar internet firibgarligining “ko‘cha jinoyatchiligi” emas, balki ma'lum intellektual va texnik tayyorgarlikni talab qiladigan jinoyat turi ekanligini tasdiqlaydi.

Internet firibgarlarining psixologik profiliga oid xalqaro tadqiqotlar ham muhim ma'lumotlarni taqdim etadi. Mazkur jinoyatchilar odatda yuqori intellektual qobiliyatga ega, kommunikativ, boshqa shaxslarda ishonch uyg‘otishga qodir, texnologik bilimlarni egallagan va risk qilishga moyil shaxslar sifatida tavsiflanadi [13].

Alohida ta'kidlash lozimki, O‘zbekistonda internet firibgarlarining muayyan mintaqaviy xususiyatlari ham kuzatilmoqda. Mamlakatda kiberjinoyatchilarning sezilarli qismi mustaqil ravishda emas, balki ijtimoiy tarmoqlardagi yopiq guruhlar va Telegram kanallari orqali tayyor firibgarlik sxemalarini o‘rganib, ularni qo‘llayotgan shaxslardir. Ya'ni, jinoyatchi doimo yuqori texnik bilimga ega bo‘lavermaydi — ba'zi hollarda tayyor zararli dasturlar va fishing shablonlari erkin sotilishi natijasida texnik jihatdan tayyorgarligi past bo‘lgan shaxslar ham bu jinoyatlarni sodir etish imkoniyatiga ega bo‘lmoqda. Hozirgi kunda kiberjinoyatchilik bozorida dastlabki kirish huquqini sotuvchi brokerlar (Initial Access Brokers) faoliyati kengayib, o‘g‘irlangan ma'lumotlar va tayyor hujum vositalari ochiq savdoga qo‘yilmoqda [14].

Kriminalistik tavsifning yana bir muhim elementi jabrlanuvchi shaxsining xususiyatlaridir. Viktimologik tahlil nafaqat sodir bo‘lgan jinoyatni tergov qilish, balki kelajakda profilaktika choralarini to‘g‘ri yo‘naltirish uchun ham zarurdir. Internet firibgarligi jabrlanuvchilari orasida muayyan ijtimoiy guruhlar alohida zaiflik ko‘rsatadi. Internet va raqamli texnologiyalar sohasida yetarli bilimlarga ega bo‘lmagan, ishonuvchan, moliyaviy qiyinchiliklarga duch kelgan yoki tez daromad olish istagida bo‘lgan shaxslar ko‘proq jabrlanmoqda. FBI IC3 2024-yilgi hisobotiga ko‘ra, 60 yoshdan oshgan fuqarolar eng ko‘p jabrlangan demografik guruh bo‘lib, ularning umumiy zarari 4,9 milliard dollarni tashkil etgan — bu ko‘rsatkich o‘tgan yilga nisbatan 43 foizga oshgan. Yosh keksalarning ko‘proq jabrlanishi ularning raqamli savodxonligining nisbatan pastligi, onlayn muhitdagi xavflarni yetarli darajada anglamasligi va ijtimoiy yolg‘izlik sababli notanish shaxslar bilan muloqotga ko‘proq moyilligi bilan izohlanadi.

BMT Inson xavfsizligi fondi ma'lumotlariga ko‘ra, O‘zbekistonda kiberjinoyatchilik jabrlanuvchilari soni 2022-yildagi 20 mingdan 2023-yilda 30 mingdan oshgan bo‘lib, moliyaviy zarar 8,5 million dollardan 25 million dollarga ko‘tarilgan, bunda yoshlar — ayniqsa ta'lim olmaydigan va ishlamaydigan yosh avlod alohida zaif guruh sifatida aniqlangan [15]. Bu ma'lumot O‘zbekistonda jabrlanuvchilar

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

tarkibining xalqaro tendensiyadan muayyan farqlanishini koʻrsatadi, ya'ni rivojlangan mamlakatlarda asosan keksa avlod jabrlansa, Oʻzbekistonda yoshlar ham jiddiy xavf guruhiga kiradi, bu esa raqamli savodxonlik dasturlarini barcha yosh guruhlarini qamrab oladigan tarzda ishlab chiqish zarurligini koʻrsatadi.

Jinoyatchi va jabrlanuvchi shaxsining kriminalistik tavsifini birgalikda tahlil qilish muhim qonuniyatni ochib beradi, ya'ni internet firibgarligida jinoyatchi va jabrlanuvchi oʻrtasida muayyan “moslik” mavjud. Jinoyatchi oʻz texnik va psixologik imkoniyatlariga qarab eng zaif toifadagi jabrlanuvchilarni maqsadli ravishda tanlaydi. Fishing hujumlarida ommaviy yoʻnalish ustunlik qilsa, investitsion va romantik firibgarlikda jinoyatchi aniq maqsadli auditoriyani - moliyaviy resurslarga ega, lekin raqamli savodxonligi past boʻlgan shaxslarni tanlaydi. Bu qonuniyatni tushunish profilaktika dasturlarini maqsadli ravishda ishlab chiqishda muhim ahamiyatga ega.

Internet firibgarligiga qarshi kurash samaradorligi koʻp jihatdan huquqiy bazaning mukammalligi, institutsional tizimning rivojlanganligi va xalqaro hamkorlik mexanizmlarining yoʻlga qoʻyilganligiga bogʻliq. Shu sababli, xorijiy davlatlarning ushbu sohadagi tajribasini qiyosiy tahlil qilish Oʻzbekiston uchun amaliy ahamiyatga ega boʻlgan xulosalar chiqarish imkonini beradi.

Amerika Qoʻshma Shtatlari internet firibgarligiga qarshi kurash tizimi eng rivojlangan modellardan biri sifatida eʻtirof etiladi. FBI tarkibidagi Internet Crime Complaint Center (IC3) 2000-yildan buyon faoliyat yuritib, fuqarolardan kiberjinoyatlarga oid shikoyatlarni qabul qilish, tahlil qilish va tergov organlari bilan muvofiqlashtirishning markazlashgan tizimini yaratgan. IC3 25-yillik faoliyati davomida 9 milliondan ortiq shikoyatni oʻz bazasida jamlagan boʻlib, faqat 2024-yilning oʻzida 859 532 ta shikoyat qabul qilingan [16]. AQSh tizimining muhim xususiyati shundaki, IC3 nafaqat shikoyatlarni yigʻadi, balki Recovery Asset Team (RAT) mexanizmi orqali firibgarlik natijasida oʻtkazilgan mablagʻlarni muzlatish va qaytarish boʻyicha operativ choralar koʻradi. 2024-yilda RAT 561,6 million dollardan ortiq firibgarlik mablagʻlarini muzlatishga muvaffaq boʻlgan. Bu tajriba shuni koʻrsatadiki, markazlashgan shikoyat tizimi va mablagʻlarni tezkor muzlatish mexanizmi birgalikda amal qilgandagina samarali natija beradi. Oʻzbekistonda esa hozircha bunday yaxlit va operativ tizim shakllanmagan. Fuqarolar shikoyatlari turli organlarga tarqoq holda kelib tushadi va mablagʻlarni muzlatish jarayoni koʻp vaqt talab qiladi.

Yevropa Ittifoqida kiberjinoyatchilikka qarshi kurash Europol tarkibidagi European Cybercrime Centre (EC3) tomonidan muvofiqlashtiriladiki, u 2013-yildan buyon faoliyat yuritib kelmoqda. EC3 ning asosiy vazifasi a'zo davlatlarning huquqni muhofaza qilish organlari oʻrtasida operativ axborot almashishni ta'minlash, transmilliy kiberjinoyatlarni tergov qilishda koʻmak koʻrsatish hamda yillik tahdid baholanmasini (IOCTA) tayyorlashdir. IOCTA

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

2024 hisobotida qayd etilishicha, Yevropa Ittifoqida kuniga millionlab fuqarolar kiberhujumlar qurboniga aylanmoqda, bunda kichik va o‘rta korxonalar kuchsiz kiberhimoya tufayli tobora ko‘proq nishonga olinmoqda. Yevropa modelining o‘ziga xos jihati shundaki, EC3 individual jinoyat ishlarini tergov qilmaydi, balki a'zo davlatlar o‘rtasida muvofiqlashtiruvchi va tahliliy funksiyani bajaradi. Bu yondashuv transmilliy xarakterga ega bo‘lgan kiberjinoyatlarni tergov qilishda samarali ekanini isbotlagan.

Buyuk Britaniya internet jinoyatlariga qarshi kurashda ikki bosqichli institutsional tizimni qo‘llaydi. National Cyber Security Centre (NCSC) milliy miqyosdagi strategik kibertahdidlarga javob berish va davlat infratuzilmasini himoya qilish vazifasini bajarsa, Action Fraud tizimi fuqarolar va kichik biznesdan firibgarlik va kiberjinoyatlarga oid shikoyatlarni qabul qilish uchun xizmat qiladi. NCSC 2024-yil sentabridan 2025-yil avgustigacha bo‘lgan davrda 204 ta milliy miqyosdagi muhim kiberhujumni bartaraf etgan bo‘lib, bu o‘tgan yilgi davrga nisbatan 129 foizlik o‘sishni ko‘rsatadi [17]. Buyuk Britaniya Hukumati tomonidan har yili o‘tkaziladigan Cyber Security Breaches Survey 2024 natijalariga ko‘ra, mamlakatdagi bizneslarning 50 foizi oxirgi 12 oy ichida kiberhujum yoki xavfsizlik buzilishiga duch kelgan, bunda fishing hujumlari eng ko‘p uchraydigan kiberjinoyat turi sifatida aniqlangan [18]. Britaniya tajribasining muhim o‘rganish kerak bo‘lgan jihati — davlat miqyosidagi kiberhimoya va fuqarolar darajasidagi shikoyat tizimi orasidagi aniq vazifa taqsimoti hamda har yilgi statistik so‘rovnomalar orqali tahdidlar manzarasini doimiy kuzatib borish amaliyotidir.

Rossiya Federatsiyasida internet firibgarligiga qarshi huquqiy baza 2012-yilda sezilarli darajada mustahkamlangan. Rossiya Federatsiyasi Jinoyat kodeksida kompyuter axboroti sohasidagi firibgarlikni — ya'ni kompyuter axborotini kiritish, o‘chirish, bloklash, o‘zgartirish yoki axborotni saqlash, qayta ishlash va uzatish vositalarining ishlashiga boshqacha aralashish orqali boshqa shaxsning mol-mulkini egallash yoki mol-mulkka bo‘lgan huquqni qo‘lga kiritishni alohida jinoyat tarkibi sifatida belgilaydi. 2018-yilda qabul qilingan 111-son Federal qonun orqali elektron to‘lov vositalari yordamidagi firibgarlik va kompyuter firibgarligi uchun javobgarlik yanada kuchaytirildi [19]. Rossiya tajribasining O‘zbekiston uchun muhim saboq bo‘ladigan jihati shuki, kompyuter firibgarligini umumiy firibgarlik moddasidan ajratib, mustaqil jinoyat tarkibi sifatida belgilash qonunchilik texnikasi jihatidan asosli yechim ekanligidadir. Biroq, Rossiyada kiberjinoyatchilik sohasida huquqni qo‘llash amaliyoti hali samarali emas. 2011-2018-yillar oralig‘ida qayd etilgan 18 333 ta kiberjinoyatdan faqat 4 100 ta jinoyatchini aniqlash mumkin bo‘lgan, bu esa qonunchilikni takomillashtirish bilan bir qatorda huquqni qo‘llash mexanizmlarini ham kuchaytirish zarurligini ko‘rsatadi.

Yuqoridagi qiyosiy tahlil bir necha muhim xulosalarni chiqarish imkonini beradi. Birinchi navbatda, internet firibgarligiga qarshi

samarali kurash markazlashgan institutsional tizimni - shikoyatlarni qabul qilish, tahlil qilish va muvofiqlashtirish funksiyalarini birlashtirgan yagona organini talab qiladi. Ikkinchidan, internet firibgarligini alohida jinoyat tarkibi sifatida qonunchilikda belgilash tergov va kvalifikatsiya jarayonini soddalashtiradi. Uchinchidan, mablag‘larni tezkor muzlatish va qaytarish mexanizmlari jabrlanuvchilar manfaatlarini himoya qilishning eng samarali vositasidir. To‘rtinchidan, yillik tahdid baholanmalari va statistik so‘rovnomalar asosida kiberjinoyatchilik manzarasini doimiy kuzatib borish strategik siyosatni shakllantirish uchun zarurdir. O‘zbekiston Respublikasi uchun ushbu tajribalarni milliy sharoitga moslashtirgan holda qo‘llash — xususan, Ichki ishlar vazirligi Kiberxavfsizlik markazi funksiyalarini kengaytirish, internet firibgarligini alohida jinoyat tarkibi sifatida Jinoyat kodeksiga kiritish va xalqaro hamkorlik mexanizmlarini mustahkamlash dolzarb masalalar sifatida kun tartibida turmoqda.

Internet firibgarligi jinoyatlarini tergov qilish an'anaviy jinoyatlarni tergovdan bir qator jiddiy jihatlar bilan farqlanadi. Mazkur jinoyatlarning raqamli muhitda sodir etilishi, jinoyatchi va jabrlanuvchining turli geografik hududlarda joylashishi, dalillarning nomoddiy xarakteri va texnologiyalarning tez sur'atda o‘zgarib borishi tergov organlarini doimiy yangi muammolar bilan yuzlantiradi. Tadqiqot doirasida tahlil qilingan jinoyat ishlari materiallari va huquqni muhofaza qilish organlari xodimlarining amaliy tajribasi asosida quyidagi asosiy muammolar aniqlandi.

Eng jiddiy to‘siqlardan biri internet firibgarligining transmilliy xarakteridir. Jinoyatchi bir davlatda, server ikkinchi davlatda, jabrlanuvchi uchinchi davlatda joylashishi mumkin, bu esa yurisdiksiya masalalarini o‘ta murakkablashtiradi. Bunday holatlarda tergov organlarining xorijiy hamkasblari bilan operativ axborot almashishi, huquqiy yordam so‘rovlarini yuborish va dalillarni topshirish jarayoni oylar, ba'zan yillar talab qiladi. O‘zbekiston IIV ma'lumotlariga ko‘ra, globallashuv va raqamlashtirish sharoitida raqamli texnologiyalar orqali sodir etiladigan jinoyatlar yildan-yilga ortib bormoqda va kiberjinoyatchilik murakkab transmilliy muammoga aylanmoqda [20]. Bundan tashqari, ko‘plab jinoyatchilar ataylab boshqa davlatlar hududidagi serverlardan va xosting xizmatlaridan foydalanadi, bu esa dalillarni olish uchun xalqaro huquqiy yordam mexanizmlarini ishga tushirishni talab qiladi. O‘zbekiston hali Yevropa Kengashining kiberjinoyatchilik to‘g‘risidagi Budapesht konvensiyasiga (2001) qo‘shilmagan bo‘lib, bu xalqaro hamkorlik imkoniyatlarini ma'lum darajada cheklaydi.

Raqamli dalillarning o‘ziga xos tabiati tergov jarayonidagi yana bir jiddiy muammodir. Elektron dalillar an'anaviy moddiy dalillardan farqli o‘laroq, oson o‘zgartirilishi, ko‘chirilishi yoki butunlay yo‘q qilinishi mumkin. Server loglari qayta yozilishi, elektron yozishmalar o‘chirilishi, soxta hisobvaraqlar yopilishi bir necha daqiqa ichida amalga oshiriladi. Shu sababli raqamli dalillarni fiksatsiya qilish vaqt

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

omili jihatidan hal qiluvchi ahamiyatga ega — jinoyat haqida xabar qilingan paytdan dalillarni yigʻish boshlangunga qadar oʻtgan har bir soat dalillar bazasining qisqarishiga olib keladi. Tadqiqot doirasida tahlil qilingan jinoyat ishlari materiallari shuni koʻrsatdiki, koʻplab hollarda jabrlanuvchilar jinoyat sodir etilganidan bir necha kun yoki hafta oʻtgandan keyin huquqni muhofaza qilish organlariga murojaat qiladi, bu vaqtga kelib esa muhim raqamli izlar allaqachon yoʻqotilgan boʻladi. Bundan tashqari, raqamli dalillarning yaxlitligini (integrity) ta'minlash — ya'ni ularning yigʻilgan paytdan sudda koʻrib chiqilgunga qadar oʻzgartirilmaganligini isbotlash alohida protsessual muammo hisoblanadi.

Tergov organlari xodimlarining raqamli kriminalistika sohasidagi bilim va koʻnikmalarining yetishmasligi muammoning institutsional tomonidir. Internet firibgarligi jinoyatlarini samarali tergov qilish tergovchidan nafaqat huquqiy, balki texnik bilimlarni — tarmoq texnologiyalari, ma'lumotlar bazalari, kriptografiya, blokchein tahlili kabi sohalar boʻyicha kompetentsiyani talab qiladi. Oʻzbekiston IIV Tergov departamenti rahbari Ramazon Ashrapovning ta'kidlashicha, huquqni muhofaza qilish organlari ilgari bu sohadagi jinoyatlarga qarshi kurashish boʻyicha yetarli tajribaga ega boʻlmagan, shu sababli vazirlik xorijiy hamkorlar bilan hamkorlikni kuchaytirish, axborot va tajriba almashishni yoʻlga qoʻyish, yetakchi xalqaro mutaxassislarni jalb qilish hamda kadrlarni tayyorlashning maxsus tizimini joriy etish zaruriyatiga duch kelgan [21]. Jahon iqtisodiy forumining Global Cybersecurity Outlook 2025 hisobotiga koʻra, tashkilotlarning uchdan ikki qismi kiberxavfsizlik sohasida oʻrta yoki jiddiy darajadagi kadrlar tanqisligini qayd etgan, faqat 14 foiz tashkilot zarur mutaxassislar va koʻnikmalarga ega ekanligiga ishonch bildirgan [22]. Bu muammo nafaqat Oʻzbekistonga, balki global miqyosda ham dolzarb boʻlib, uning yechimi uzluksiz kadrlar tayyorlash tizimini yaratishni talab qiladi.

Yuqoridagi muammolarga qoʻshimcha ravishda, amaliyotda protsessual tartibning raqamli dalillar xususiyatlariga moslashtirilmaganligi ham jiddiy toʻsiq boʻlib qolmoqda. Amaldagi jinoyat-protsessual qonunchilikda raqamli dalillarni yigʻish, saqlash va ekspertiza qilish tartibi yetarli darajada tartibga solinmagan. Masalan, serverdan ma'lumotlarni olib qoʻyish (imaging), xesh-summa orqali dalilning yaxlitligini tasdlqlash, bulutli xizmatlardan dalil olish kabi masalalar protsessual jihatdan aniq belgilanmagan. Bu holat tergov davomida toʻplangan dalillarning sudda rad etilishi xavfini oshiradi va tergov samaradorligini pasaytiradi. Shu boisdan, raqamli dalillar bilan ishlash boʻyicha yagona milliy standart va metodologik koʻrsatmalar ishlab chiqish — bu nafaqat nazariy, balki oʻta amaliy zaruriyat hisoblanadi.

Ushbu maqolada internet tarmogʻida sodir etiladigan firibgarlik jinoyatlarining kriminalistik tavsifi har tomonlama oʻrganildi. Olingan natijalar asosida quyidagi xulosalar shakllantirildi:

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Birinchidan, internet firibgarligi oʻzining texnik murakkabligi, anonimlik imkoniyatlari va transmilliy xarakteri bilan an'anaviy firibgarlikdan sifat jihatidan farqlanuvchi mustaqil jinoyat turi sifatida namoyon boʻladi. Jinoyatchi va jabrlanuvchining yuzma-yuz muloqotsiz, raqamli muhit orqali oʻzaro ta'siri bu jinoyat turiga kriminalistik jihatdan alohida yondashish zarurligini belgilaydi.

Ikkinchidan, internet firibgarligi jinoyatlarining kriminalistik tavsifi quyidagi oʻzaro bogʻliq elementlardan iborat yaxlit tizimni tashkil etadi: jinoyatning predmeti va obyekti, sodir etilish mexanizmi (tayyorgarlik, amalga oshirish va yashirish bosqichlari), raqamli izlar tizimi, jinoyatchi shaxsining tipologiyasi va jabrlanuvchi shaxsining viktimologik xususiyatlari. Ushbu elementlarning yaxlit tizim sifatida oʻrganilishi tergov versiyalarini ilgari surish va dalillar bazasini shakllantirish samaradorligini oshiradi.

Uchinchidan, jinoyat sodir etilishining uch bosqichli mexanizmi — tayyorgarlik, amalga oshirish va yashirish — har bir bosqichda oʻziga xos kriminalistik ahamiyatga ega raqamli izlar qoldiradi. Ayniqsa tayyorgarlik bosqichida qoldirilgan domen registratsiyasi ma'lumotlari, xosting xizmati qaydlari, VPN provayderga toʻlov tarixi va soxta sayt metadata ma'lumotlari jinoyatchini aniqlashda hal qiluvchi dalil boʻlib xizmat qilishi mumkin. Raqamli izlarning oson yoʻq qilinishi sababli ularni oʻz vaqtida fiksatsiya qilish tergov muvaffaqiyatining asosiy sharti hisoblanadi.

Toʻrtinchidan, internet firibgarlarining tipologik tavsifi shuni koʻrsatadiki, ularning taxminan 65 foizi 20—35 yoshli, 78 foizi erkak, 70 foizdan ortigʻi oliy yoki oʻrta maxsus ma'lumotli, axborot texnologiyalari yoki moliya sohasida muayyan bilimga ega shaxslardan iborat. Biroq zamonaviy sharoitda tayyor zararli dasturlar va fishing shablonlarining erkin tarqalishi texnik tayyorgarligi past boʻlgan shaxslarga ham bu jinoyatlarni sodir etish imkonini bermoqda, bu esa jinoyatchilar doirasini kengaytirmoqda.

Beshinchidan, AQSh, Yevropa Ittifoqi, Buyuk Britaniya va Rossiya Federatsiyasi tajribasining qiyosiy tahlili Oʻzbekiston uchun bir necha muhim amaliy ishlarni oʻz ichiga oladi: shikoyatlarni qabul qilish, tahlil qilish va muvofiqlashtirish funksiyalarini birlashtirgan markazlashgan institutsional tizim zaruriyati; internet firibgarligini alohida mustaqil jinoyat tarkibi sifatida Jinoyat kodeksida belgilash maqsadga muvofiqligi; firibgarlik mablagʻlarini tezkor muzlatish mexanizmini joriy etish kabilar.

Oltinchidan, tergov amaliyotidagi asosiy muammolar sifatida quyidagilar jinoyatlarning transmilliy xarakteri va yurisdiksiya masalalari; raqamli dalillarning oʻzgaruvchan va tez yoʻq qilinadigan tabiati; VPN, Tor tarmogʻi va kriptovalyutalar orqali ta'minlanadigan anonimlik; tergov organlari xodimlarining raqamli kriminalistika sohasidagi bilim va koʻnikmalarining yetishmasligi; hamda amaldagi jinoyat-protsessual qonunchilikda raqamli dalillar bilan ishlash tartibining yetarli darajada tartibga solinmaganligi aniqlandi.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Yuqoridagi xulosalar asosida quyidagi taklif va tavsiyalar ilgari suriladi:

O‘zbekiston Respublikasi Jinoyat kodeksiga internet firibgarligini an'anaviy firibgarlikdan ajratib, axborot-kommunikatsiya texnologiyalari orqali sodir etilgan firibgarlik uchun alohida javobgarlikni nazarda tutuvchi mustaqil modda kiritish maqsadga muvofiq**.** Bu tergov va sudlov amaliyotida kvalifikatsiya masalalarini soddalashtiradi. ghgh

Raqamli dalillarni yig‘ish, saqlash, ekspertiza qilish va sudda taqdim etish tartibini belgilovchi yagona milliy standart va metodologik ko‘rsatmalar ishlab chiqilishi zarur. Xususan, serverdan ma'lumotlarni olib qo‘yish, xesh-summa orqali dalil yaxlitligini tasdiqlash va bulutli xizmatlardan dalil olish masalalari protsessual jihatdan aniq tartibga solinishi lozim.

Internet jinoyatlariga oid shikoyatlarni markazlashgan holda qabul qilib, tahlil qilish va operativ choralar ko‘rish imkonini beradigan maxsus platforma tashkil etilishi tergov jarayonining samaradorligini oshiradi.

O‘zbekiston Respublikasining Yevropa Kengashining kiberjinoyatchilik to‘g‘risidagi Budapesht konvensiyasiga qo‘shilishi transmilliy jinoyatlarni tergov qilishda xalqaro hamkorlik imkoniyatlarini sezilarli darajada kengaytiradi.

Tergov organlari xodimlarini raqamli kriminalistika, blokcheyn tahlili, kompyuter tarmoqlari va elektron dalillar sohasida muntazam qayta tayyorlash tizimini joriy etish, shuningdek, universitetlar va vazirliklar o‘rtasida amaliy hamkorlikni yo‘lga qo‘yish tavsiya etiladi.

Xulosa qilib aytganda, internet firibgarligi jinoyatlarining kriminalistik tavsifini o‘rganish nafaqat nazariy, balki tergov amaliyotini takomillashtirish uchun bevosita amaliy ahamiyatga ega. Raqamli texnologiyalarning jadal rivojlanishi va kiberjinoyatchilarning yangi usullarga — sun'iy intellekt, deepfake texnologiyalariga ko‘proq murojaat qilayotganligi kriminalistika fanining mazkur sohadagi tadqiqotlarni uzluksiz davom ettirishini va huquqiy bazaning doimiy yangilanib borishini taqozo etadi. O‘zbekiston uchun ushbu yo‘nalishdagi tadqiqotlar milliy kiberhimoya tizimini mustahkamlashning ilmiy asosini tashkil etadi.

REFERENCES

1. Morgan, S. (2024, June 24). 2024 Cybersecurity Almanac: 100 facts, figures, predictions and statistics. Cybercrime Magazine / Cybersecurity Ventures.

2. Fleck, A. (2024, February 22). Cybercrime expected to skyrocket in coming years [Infographic]. Statista.

3. Federal Bureau of Investigation. (2025). 2024 Internet Crime Report. Internet Crime Complaint Center (IC3).

4. LevelBlue. (2025, April 25). FBI 2024 IC3 report: Phishing soars, ransomware batters critical infrastructure as cyber losses climb. LevelBlue Blog.

5. Ogbara, B. (2024, July 26). Europol‘s 2024 IOCTA report. Digital Asset Redemption.
6. Gazeta.uz. (2025, May 31). Cybercrimes in Uzbekistan increase 68-fold in five years.
7. Kun.uz. (2025a, February 27). Crime rate in Uzbekistan: MIA reports nearly 200 offenses per 100,000 people for 2024.
8. YUZ.uz. (2025, May 30). In Uzbekistan, the number of cybercrimes has increased 68-fold over the past five years.
9. TRM Labs. (2025, April 23). A record-breaking year for cybercrime: Key findings from the FBI‘s 2024 IC3 report. TRM Blog.
10. California Department of Financial Protection and Innovation. (n.d.). Pig butchering – how to spot and report the scam. DFPI. Retrieved March 1, 2026, from
11. Kun.uz. (2025b, February 3). Over 12 million cyberattacks recorded in Uzbekistan in 2024.
12. Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union.
13. Holt, T.J. & Bossler, A.M. Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses. Routledge, 2016. URL:
14. Help Net Security. (2025, June 12). Cybercriminals are turning stolen data into a thriving black market.
15. United Nations Human Security Unit. (2025, April 25). Strengthening resilience of youth to cybercrime and digital violence in Uzbekistan. United Nations.
16. Federal Bureau of Investigation. (2025, April 24). FBI releases annual Internet crime report [Press release].
17. Watson, M. (2026, January 16). UK cybercrime reports surge as true costs hidden. SecurityBrief UK.
18. Department for Science, Innovation and Technology. (2024, April 9). Cyber security breaches survey 2024. GOV.UK.
19. Sukharenko, A. (2019, July 8). Russian ITC security policy and cybercrime (PONARS Eurasia Policy Memo No. 601). PONARS Eurasia.
20. Ministry of Internal Affairs of the Republic of Uzbekistan. (2025, May 7). Creating a safe cyberspace by combating cybercrime: Uzbekistan‘s experience in the early prevention of cybercrime in the context of digital transformation. Government Portal of the Republic of Uzbekistan.
21. The Caspian Post. (2025, December 23). Uzbekistan sees massive rise in cybercrime cases. Caspianpost.com.
22. World Economic Forum. (2025, January). Global cybersecurity outlook 2025. In collaboration withAccenture.