

**AXBOROT TEXNOLOGIYALARIDAN FOYDALANIB SODIR ETILGAN
FIRIBGARLIK JINOYATIDA ANIQLANISHI LOZIM BO'LGAN
HOLATLAR**

Nosirov Amirxon Bahodir o'g'li

Toshkent davlat yuridik universiteti

*12.00.09 - Jinoyat protsessi. Kriminalistika, tezkor-qidiruv huquq va sud
ekspertizasi ixtisosligi mustaqil izlanuvchisi*

ANNOTATSIYA

Ushbu tezisda axborot texnologiyalaridan foydalanib sodir etilgan firibgarlik jinoyatlarini tergov qilish jarayonida aniqlanishi lozim bo'lgan holatlar ilmiy-huquqiy hamda kriminalistik nuqtai nazardan tizimli tahlil etiladi. Tadqiqot O'zbekiston Respublikasi Jinoyat-protsessual kodeksining 82–83-moddalari, Jinoyat kodeksining 168-moddasi, shuningdek, 2001-yilgi Kiberjinoyatchilik to'g'risidagi Budapesht konvensiyasi normalari asosida olib borilgan.

Tezisda kiberfiribgarlik jinoyatlarida isbotlash predmeti an'anaviy jinoyat turlaridan mazmun va ularni aniqlash usullari jihatidan tubdan farq qilib, raqamli dalillar bazasini mustahkamlash va tergov samaradorligini ta'minlash uchun protsessual-huquqiy hamda kriminalistik holatlarning integratsiyalashgan tizimini qo'llash zarurligi bayon etiladi.

Kalit so'zlar: axborot texnologiyalari, kiberfiribgarlik, isbotlash predmeti, tergov metodologiyasi, raqamli izlar, Budapesht konvensiyasi, raqamli dalillar.

Kirish

Kriminalistika fanining fundamental qoidalariga ko'ra, har bir jinoyat o'zining kelib chiqishi va sodir etilish mexanizmiga ko'ra individual xarakterga ega. Biroq, muayyan turdagi qilmishlarga xos bo'lgan ayrim o'xshash elementlar va qonuniyatlar ilgari sodir etilgan jinoyat izlari hamda usullari bilan umumiy jihatlarga ega bo'lishi yoki aksincha, mutlaqo o'ziga xos jihatlari namoyon bo'lishi mumkin.

Amaldagi jinoyat-protsessual qonuni normalariga ko'ra, tergovchi yoki surishtiruvchi har qanday sodir etilgan jinoyat haqidagi xabarni qabul qilishi, har tomonlama tekshirishi va qonun hujjatlarida ko'rsatilgan qat'iy muddatlar ichida qonuniy to'xtamga kelishi majburiydir. Tergovga qadar tekshirish jarayoni faqatgina ma'lum bo'lgan dastlabki jinoiy faktlarni tekshirish bilan cheklanib qolmay, yangi jinoiy holatlarni yuzaga chiqarish xususiyatiga ham ega. Axborot texnologiyalaridan foydalanib sodir etilgan firibgarlik jinoyatida aniqlanishi lozim bo'lgan holatlar tergov

jarayonining metodologik asosini tashkil etadi. O'zbekiston Respublikasi Jinoyat-protsessual kodeksining 82-moddasida isbotlash predmeti ya'ni har bir jinoyat ishida aniqlanishi shart bo'lgan holatlar ro'yxati mustahkamlangan.

Kriminalistika fanining yirik namoyandalaridan biri R.S. Belkin tergov jarayonida aniqlanishi lozim bo'lgan holatlarni tizimli ravishda ikki qatlamga ajratadi: birinchi qatlam jinoyat-protsessual qonunchiligida mustahkamlangan va barcha jinoyat toifalari uchun umumiy hisoblangan isbotlash predmeti; ikkinchi qatlam esa muayyan jinoyat turining kriminalistik tavsifidan kelib chiquvchi, faqat o'sha guruhga mansub qilmishlar uchun xarakterli bo'lgan maxsus holatlardir¹. Professor R.S. Belkin ta'kidlaganidek, axborot texnologiyalari vositasida sodir etiladigan firibgarlik jinoyatlarini tergov qilish metodologiyasini ishlab chiqishda ushbu ikki qatlamning o'zaro integratsiyasini ta'minlash konseptual ahamiyatga ega. Zero, protsessual va kriminalistik xarakterdagi holatlar yagona tizimda, kompleks tarzda tadqiq etilgandagina, kiberfiribgarlik jinoyatlari bo'yicha dastlabki tergovning yuqori samaradorligi va qonuniyligini kafolatlash mumkin.

Taniqli kriminalist olim V.A. Obratsov o'zining ilmiy tadqiqotlarida jinoyatlarni tergov qilish uslubiyotida isbotlanishi shart bo'lgan holatlarni to'rtta fundamental turkumga ajratishni taklif etadi. Ushbu tasnif tizimiga muvofiq, muvaffaqiyatli tergovni amalga oshirish uchun tergovchining diqqat markazida bevosita jinoyat hodisasi, jinoyatchining shaxsiy xususiyatlari, qilmish oqibatida yuzaga kelgan zarar ko'lami hamda jinoyat sodir etilishiga yo'l ochgan omillar tahlili turishi lozim. Mazkur guruhlarining tizimli o'rganilishi kiberjinoyatlar va an'anaviy jinoyatlarni fosh etish metodikasini to'g'ri shakllantirishga xizmat qiladi².

O'zbekiston Respublikasi Jinoyat-protsessual kodeksining 82-moddasida belgilangan 7 ta holat ham ushbu to'rt guruh doirasida joylashadi va ushbu turdagi uchun aniq mazmun kasb etadi.

Kiberfiribgarlik jinoyatlarini tergov qilishda aniqlanishi lozim bo'lgan holatlarning birinchi guruhi, ya'ni jinoyat hodisasining tarkibiy elementlari mazkur jinoiy qilmish turida mutlaqo yangicha kriminalistik mazmun va mohiyat kasb etadi. Ushbu turkum doirasida, eng avvalo, jinoyatning sodir etilish vaqti, joyi va usuli kabi fundamental holatlar aniqlanishi talab etiladi. Biroq, klassik (an'anaviy) jinoyatlardan farqli o'laroq, axborot texnologiyalari sohasidagi tajovuzlar muayyan geografik makon bilan cheklanmasdan, virtual muhitda kechadi va transchegaraviy xarakterga ega bo'lib, bir vaqtning o'zida bir nechta davlatlar hududini qamrab olishi mumkin. Shu bois, kiberolamda jinoyatning sodir etilish joyini moddiy koordinatalar bo'yicha emas,

¹Белкин Р. С. Курс криминалистики : в 3 т. М. : Юристъ, 1997. Т. 2. С. 444..

²Криминалистика : учебник для вузов / В. А. Образцов [и др.] ; под ред. В. А. Образцова. — М. : Юристъ, 1995. — 760 с.

balki qilmishga vosita bo'lgan muayyan server, tarmoq infratuzilmasi yoki raqamli platformani ixtisoslashtirilgan kompyuter-texnik tahlil etish orqali identifikatsiya qilish lozim.

Kiberfiribgarlik jinoyatlarining sodir etilish mexanizmi, xususan, jabrlanuvchiga nisbatan qo'llaniladigan aldash va ishonchni suiste'mol qilish usullari ham mazkur kriminalistik guruhning tarkibiy qismi sifatida tadqiq etiladi. Ushbu toifadagi jinoyatlarda qo'llaniladigan asosiy usullarni quyidagicha tasniflaydi va tavsiflaydi: fishing (soxta veb-saytlar hamda resurslar orqali konfidentsial va shaxsiy ma'lumotlarni g'ayriqonuniy o'g'irlash), vishing (telefon qo'ng'iroqlari va ovozli aloqa vositasida aldash), smishing (SMS-xabarnomalar orqali chalg'itish), spoofing (tarmoq identifikatorlari va texnik ma'lumotlarini soxtalashtirish) hamda ijtimoiy muhandislik (ijtimoiy-psixologik manipulyatsiya yordamida aldash).

2001-yildagi Kiberjinoyatchilik to'g'risidagi Budapesht konvensiyasining 8-moddasida kompyuter texnikasi vositasida sodir etiladigan firibgarlik qilmishining konstruktiv elementlari belgilangan bo'lib, mazkur xalqaro-huquqiy standart jinoyat hodisasiga daxldor bo'lgan va tergov jarayonida aniqlanishi lozim bo'lgan holatlar tizimini shakllantirishda fundamental metodologik mezon vazifasini bajaradi. Kriminalist olim ushbu sohada yetuk mutaxassislardan bo'lgan E.Keysining ta'kidlashicha, ushbu toifadagi kiberjinoyatlarning sodir etilish usulini aniqlash ko'pincha moliyaviy tranzaksiyalar ma'lumotlari, server log-fayllari (tizim jurnallari) hamda elektron pochta sarlavhalarini (headers) kompleks raqamli tahlil etish orqali amalga oshiriladi. Zero, aynan mana shunday kompleks kriminalistik tahlil virtual makonda yuz bergan jinoiy mexanizmning yaxlit va izchil retrospektiv modelini shakllantirish imkonini beradi³.

Tergov jarayonida aniqlanishi shart bo'lgan holatlarning ikkinchi guruhi — aybdor shaxsning kriminologik xarakteristikasi bo'lib, u kiber-muhitdagi jinoyatlarda klassik jinoyat turlariga qaraganda mutlaqo boshqacha (spetsifik) mazmun kasb etadi. Olim N.G. Shuruxnovning qayd etishicha, kibermakondagi jinoyatchilarni fosh etish va shaxsini aniqlashda yetarli texnik va raqamli malakaga ega bo'lmagan tergovchilar jiddiy to'siqlarga duch kelishadi. Buning asosiy sababi, jinoiy subyektlarning yashirin faoliyat yuritishi hamda o'zlarining haqiqiy identifikatorlarini yashirish maqsadida turli ko'p bosqichli anonimlashtirish vositalaridan keng foydalanishidir⁴.

Kiber-muhitda sodir etilgan jinoyatlar ijrochilarini aniqlash raqamli izlarni, jumladan, IP-manzillar (Internet Protocol address), MAC-manzillar (Media Access Control address), SIM-karta raqamlari, virtual foydalanuvchi profillari, raqamli

³Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Waltham: Academic Press, 2011. B. 163–175.

⁴Шурухнов Н.Г. Криминалистика: учебник. М.: Юрист, 2004. 639 с.

imzolar hamda qurilmaning xalqaro identifikatsiya kodlari (IMEI) kabi elektron identifikatorlar majmuasi chuqur tahlil etiladi. Mazkur raqamli identifikatorlarning har biri alohida olinganda jinoiy subyektning shaxsini to'liq va so'zsiz isbotlash imkoniga ega bo'lmasa-da, ularning o'zaro tizimli korrelyatsiyasi hamda integratsiyalashgan majmuasi ish bo'yicha yagona, rad etib bo'lmas va ishonchli elektron dalillar bazasini shakllantiradi⁵.

Jinoyatchi shaxsiga oid holatlar doirasida yana quyidagilar aniqlanishi lozim: jinoyatchi yoki jinoyatchilar guruhining texnik bilim va ko'nikma darajasi (bu holat qo'llangan usulning murakkabligi va oldindan rejalashtirilganligini ko'rsatadi), ular tomonidan foydalanilgan anonimlashtiruvchi vositalar (VPN, Tor tarmog'i, proxy-serverlar), guruhda harakat qilganlik va rollarning taqsimlanishi, hamda jinoyatning qaysi davlatdan turib sodir etilganligi.

Ushbu yo'nalishda ko'zga ko'ringan mutaxassis E. Keysi qayd etganidek, raqamli izlar server log-fayllarida qayta tiklanishi mumkin bo'lgan barqaror formatda saqlanib qoladi. Binobarin, jinoyatchi o'z harakatlarining elektron izlarini o'chirishga faol uringan taqdirda ham, kriminalistik tahlillar va maxsus uslublar yordamida rad etib bo'lmaydigan dalillarni aniqlash va kiberjinoyatni fosh etish mexanizmini amalga oshirish mumkin bo'ladi⁶.

Kiberfiribgarlik ishlari bo'yicha aniqlanishi lozim bo'lgan holatlarning uchinchi guruhi bevosita jinoyat oqibatlari va jabrlanuvchi shaxsi bilan bog'liqdir. Mazkur guruh doirasidagi tergov harakatlarining ustuvor yo'nalishi sifatida, dastlab, jabrlanuvchi jismoniy yoki yuridik shaxslarga yetkazilgan moddiy zararining aniq miqdorini tahlil etish va belgilash talab etiladi.

O'zbekiston Respublikasi Jinoyat-protsessual kodeksining 82-moddasi birinchi qismining 5-bandida qonuniy jihatdan mustahkamlab qo'yilganidek, jinoyat natijasida yetkazilgan mulkiy va boshqa zararining miqdori hamda xarakteri (tabiati) har bir jinoyat ishi bo'yicha tergov jarayonida majburiy tartibda aniqlanishi shart bo'lgan mustaqil holat (isbotlash predmeti) hisoblanadi. Mazkur toifadagi kiberfiribgarlik jinoyatlarida jinoiy tajovuz oqibatida yetkazilgan moddiy zararining real ko'lamini belgilash elektron to'lov tizimlarida amalga oshirilgan operatsiyalar, bank muassasalarining tranzaksiyaviy yozuvlari (log-fayllari), virtual raqamli hamyonlar tarixi hamda kripto-aktivlar harakati traektoriyasini chuqur kriminalistik va sud-iqtisodiy ekspertizaviy tahlil etish orqali amalga oshiriladi.

Shu bilan birga, jinoiy oqibatlarni isbotlash predmetining ajralmas qismi sifatida jabrlanuvchining shaxsiga oid individual xususiyatlarni, xususan, uning axborot

⁵Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Waltham: Academic Press, 2011.

texnologiyalari va kiber-gigiyena sohasidagi raqamli savodxonlik hamda viktimallik darajasini kompleks aniqlash jinoyat metodologiyasini to'g'ri baholash imkonini beradi.

Ushbu holatni o'rganish ikki asosiy sababga ko'ra zarurdir. Birinchidan, bu jinoyatchi tomonidan ishlatilgan aldash usullarining jabrlanuvchiga qanday ta'sir qilganini kriminalistik nuqtayi nazardan tushuntirib beradi. Ikkinchidan, jinoiy qilmishga to'g'ri huquqiy baho berishda, ya'ni aybdor shaxs jabrlanuvchining raqamli savodxonligi pastligidan ataylab foydalanganini isbotlashda muhim dalil bo'ladi⁷. Aynan shu bois, O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasida firibgarlik jinoyatini malakalashda jabrlanuvchining zaif holatidan foydalanish va katta miqdordagi zarar yetkazish holatlari alohida javobgarlikni og'irlashtiruvchi belgilar sifatida to'g'ridan-to'g'ri ko'rsatib o'tilgan.

Isbotlash predmeti tarkibidagi to'rtinchi guruh jinoyat izlariga oid holatlar mazkur toifadagi kiberfiribgarliklarning eng o'ziga xos, o'zak xususiyatini tashkil etadi va ushbu guruhning strukturaviy-mazmuniy tabiati klassik (an'anaviy) firibgarlik shakllaridan tubdan farq qiladi. Kriminalistik ma'noda raqamli izlar (digital traces) bu bevosita inson a'zolari orqali vizual idrok etib bo'lmaydigan, biroq maxsus dasturiy-texnik vositalar yordamida aniqlanishi, o'qilishi va retrospektiv tarzda qayta tiklanishi mumkin bo'lgan o'ziga xos elektron ma'lumotlar majmuasidir.

Raqamli kriminalistika sohasining taniqli olimi E. Keysi raqamli izlarning quyidagi fundamental turlarini tasniflaydi: server tizim jurnallarida (log-fayllarda) muhrlangan ulanish va autentifikatsiya ma'lumotlari, veb-brauzerlar tarixi va kesh-xotira fragmentlari, elektron pochta sarlavhalari (headers) hamda ularning tarkibiy qismlari, elektron to'lov va bank tizimlari orqali amalga oshirilgan tranzaksiyalar tarixi, mobil qurilmalarning geografik joylashuviga oid koordinatalar (GPS yoki mobil aloqa operatorlarining baza stansiyalari ma'lumotlari), virtual ijtimoiy tarmoqlardagi faollik qaydlari hamda zararli dasturiy ta'minotlar (malware) tomonidan qoldirilgan raqamli artefaktlar⁸.

Bugungi raqamli transformatsiya davrida ushbu nazariy qarashlar Kiberjinoyatchilik bo'yicha Budapesht konvensiyasining 16–17-moddalarida mustahkamlangan virtual ma'lumotlarni tezkor saqlash va muhofaza qilish tartiblari bilan uzviy bog'lanadi. Kiber-muhitda qoldirilgan elektron izlarni to'g'ri protsessual rasmiylashtirish ularning sudda yuridik kuchga ega bo'lgan raqamli dalil sifatida tan olinishini kafolatlaydi. Shuning hisobiga, hozirgi tergov amaliyotida raqamli

⁶Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Waltham: Academic Press, 2011.

dalillarning o'zgartirilmaganligi (yaxlitligi) va haqiqiyliigi (autentikligi) masalasini qat'iy tekshirish kiber-tergov muvaffaqiyatini belgilovchi bosh mezonga aylanmoqda⁹.

Isbotlash predmeti tarkibidagi beshinchi guruh — jinoyat sodir etilishiga imkon bergan sabablar va sharoitlarni aniqlashga doir talablar O'zbekiston Respublikasi Jinoyat-protsessual kodeksining 82-moddasi 7-bandida qonuniy jihatdan mustahkamlangan. Mazkur toifadagi kiberfiribgarlik jinoyatlari bo'yicha qo'zg'atilgan ishlar doirasida ushbu guruh doirasida quyidagi fundamental determinat va omillar tizimli ravishda aniqlanishi lozim: axborot-kommunikatsiya tizimlari xavfsizligidagi xarakterli texnik defektlar (zaif autentifikatsiya parollari, o'z vaqtida yangilanmagan dasturiy ta'minot, kriptografik shifrlash bayonnomalarining mavjud emasligi); subyektlarning raqamli va kiber-savodxonlik darajasi pastligi oqibatida manipulyatsiyalarga (aldanishga) moyilligi (viktimologik omil); xo'jalik yurituvchi subyektlar hamda tashkilotlarda axborot xavfsizligini ta'minlash mexanizmlarining destabilligi va xodimlar o'rtasida preventiv-profilaktika tadbirlarining korporativ darajada olib borilmasligi; shuningdek, elektron moliyaviy tizimlar va bank sektorida tranzaksiyalar monitoringi (anti-frod tizimlari) samaradorligining pastligi hamda amaldagi qonunchilik bazasidagi reguliyativ bo'shliqlar.

Axborot texnologiyalari sohasidagi firibgarliklarga imkon beruvchi omillarni texnik, tashkiliy va insoniy (subyektiv) guruhlariga ajratib, ularning har biriga qarshi maqsadli profilaktika chora-tadbirlarini amalga oshirish lozimligini ta'kidlaydi. Kiber-muhitdagi global tahdidlarni tahlil qiluvchi Europolning «IOCTA 2021» hisoboti ham ushbu fikrni qo'llab-quvvatlab, onlayn firibgarliklarning o'sishiga profilaktik monitoringning sustligi hamda aholining raqamli savodxonligi yetarli emasligi sabab bo'layotganini qayd etadi. Shu bois, jinoyatning sodir etilishiga yordam bergan sabab va sharoitlarni aniqlash shunchaki tergov vazifasi emas, balki kelajakda o'xshash jinoyatlarning barvaqt oldini olish tizimining ajralmas qismidir. Tergov organi muayyan ish bo'yicha kamchiliklarga yo'l qo'ygan korxona yoki idoralarga taqdimnomalar kiritish orqali jinoyat-protsessual qonunchiligida belgilangan preventiv (profilaktika) vazifasini amalda muvaffaqiyatli realizatsiya qiladi.

Ushbu turdagi jinoyatida aniqlanishi lozim bo'lgan holatlar tizimini nazariy jihatdan tahlil qilish shuni ko'rsatadiki, ushbu holatlar an'anaviy firibgarlik uchun belgilangan holatlardan nafaqat mazmun, balki ularni aniqlash usullari jihatidan ham tubdan farq qiladi. R.S.Belkin nazariyasiga muvofiq, jinoyat-protsessual qatlamdagi umumiy holatlar (JPK 82-modda) va kriminalistik qatlamdagi maxsus holatlar (jinoyatning kriminalistik tavsifidan kelib chiqqan holatlar) o'zaro

⁹Budapesht Convention. ETS No. 185. Art. 16–17 (Expedited preservation of stored computer data and traffic data)

uyg'unlashtirilgandagina isbotlash predmeti to'liq hisoblanadi¹⁰. V.A.Obraztsovning metodologik tasnifi esa ushbu holatlarni amaliy tergov jarayonida guruhlab ishlash imkonini beradi: har bir guruh bo'yicha aniqlanishi zarur bo'lgan holatlar ro'yxatini oldindan belgilash, ularni aniqlash uchun zarur tergov harakatlari ketma-ketligini rejalashtirish va natijalarni tizimli ravishda umumlashtirish tergov samaradorligini sezilarli darajada oshiradi¹¹.

O'zbekiston Respublikasi Jinoyat-protsessual kodeksining 83-moddasida isbotlash predmetining elementlari batafsil belgilangan bo'lib, ushbu elementlarning ushbu turdagi ishlarida qo'llanilishi o'ziga xos kriminalistik mazmun kasb etadi. Jinoyat hodisasi (sodir etilgan joyi, vaqti, usuli) ushbu turdagida virtual muhitda aniqlanadi; aybdorlik raqamli identifikatsiya orqali isbotlanadi; jazo tayinlashga ta'sir etuvchi holatlar uyushgan guruh, katta miqdorda zarar va ilgari sudlanganligi kabi belgilar Ushbu turdagi uchun ham amaliy ahamiyat kasb etadi; yetkazilgan zarar moliyaviy tranzaksiyalar tahlili orqali aniqlanadi.

Xalqaro huquqiy asoslar nuqtai nazaridan Budapesht Konventsiyasining 2–11-moddalarida kiberjinoyatlarni tashkil etuvchi elementlar belgilangan bo'lib, ushbu elementlar ushbu turdagi uchun aniqlanishi lozim bo'lgan holatlarning xalqaro mezonini tashkil etadi¹². N.G.Shuruxnov ta'kidlaganidek, Ushbu turdagi tergovda maxsus texnik bilimlardan foydalanish zarurati isbotlash predmetini to'liq qamrab olishning zaruriy shartidir: texnik ekspertsiz raqamli izlarni aniqlash, moliyaviy tranzaksiyalar zanjirini kuzatish va jinoyatchi shaxsini raqamli yo'l bilan identifikatsiya qilish deyarli mumkin emas¹³. Shunday qilib, Ushbu turdagi uchun aniqlanishi lozim bo'lgan holatlar tizimi O'zbekiston Respublikasi Jinoyat-protsessual kodeksining 82-83-moddalarida belgilangan umumiy holatlar bilan xalqaro standartlar va kriminalistik fan talablarini birlashtirgan, besh guruhdan iborat kompleks tizim sifatida shakllantirilishi lozim.

O'zbekiston qonunchiligida Ushbu turdagi uchun alohida kriminallashtirishning yo'qligi aniqlanishi lozim bo'lgan holatlar tizimini shakllantirishda ham ma'lum muammolarni yuzaga keltiradi. O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasida firibgarlik uchun umumiy javobgarlik belgilangan bo'lib, axborot texnologiyalari orqali sodir etilishi alohida malakashtiruvchi belgi sifatida ko'rsatilmagan. Bu holat tergovchi va sudyalalar uchun ushbu turdagi uchun aniqlanishi lozim bo'lgan holatlar ro'yxatini shakllantirishni qiyinlashtiradi.

⁸Белкин Р.С. Курс криминалистики. В 3-х т. Т.3: криминалистические средства, приемы и рекомендации.-м.: юристъ,1997.- 480 с.

⁹Криминалистика : учебник для вузов / В. А. Образцов [и др.] ; под ред. В. А. Образцова. — М. : Юристъ, 1995. — 760 с.

¹⁰Budapesht Convention. ETS No. 185. Art. 2–11 (Substantive criminal law)

¹¹Шурухнов Н.Г. Криминалистика: учебник. М.: Юрист, 2004. 639 с.

Xulosa

Xulosa o'rnida ta'kidlash lozimki, kiberfiribgarlik jinoyatlarida aniqlanishi shart bo'lgan holatlar tizimi (jinoyat voqeasi, jinoyatchi shaxsining kriminologik tavsifi, jabrlanuvchining viktimologik xususiyatlari, virtual makondagi izlar hamda jinoyatga zamin yaratgan omillar) klassik firibgarlik turlaridan butunlay farq qiladi va o'ziga xos raqamli-kriminalistik mazmunga egadir. Ushbu holatlarni to'liq, kompleks va o'zaro uzviy zanjirda aniqlash zamonaviy tergov jarayonlarining muvaffaqiyatini ta'minlovchi asosiy omil hisoblanadi. Bu esa, o'z navbatida, raqamli dalillar bazasini mustahkamlashga va jinoyat sodir etgan shaxslarni adolat tamoyillari asosida javobgarlikka tortishga bevosita zamin yaratadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasi Jinoyat kodeksi. 1994 yil 22 sentyabr, № 2012 XIIson. Toshkent: Adolat, 2024-yil nashri.
2. O'zbekiston Respublikasi Jinoyat-protsessual kodeksi. 1994 yil 22 sentyabr, № 2013-XII-son. Toshkent: Adolat, 2024-yil nashri.
3. O'zbekiston Respublikasi Prezidentining 2020 yil 5 oktyabrdagi PF-6079-son Farmoni "2030 yilgacha bo'lgan davrda O'zbekistonda raqamli iqtisodiyotni rivojlantirish strategiyasini tasdiqlash to'g'risida"
4. Council of Europe Convention on Cybercrime (Budapesht Convention). ETS No. 185. Budapesht, 23 November 2001. URL: <https://www.coe.int>
5. Financial Action Task Force (FATF). International Standards on Combating Money Laundering: The FATF Recommendations. Paris: FATF/OECD, 2020.
6. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2021. The Hague: Europol Publication Office, 2021.
7. Белкин Р. С. Курс криминалистики : в 3 т. М. : Юристъ, 1997. Т. 2. С. 444.
8. Белкин Р.С. Курс криминалистики. В 3-х т. Т.3: криминалистические средства, приемы и рекомендации.-м.: юристъ,1997.- 480 с.
9. Криминалистика : учебник для вузов / В. А. Образцов [и др.] ; под ред. В. А. Образцова. — М. : Юристъ, 1995. — 760 с.
10. Шурухнов Н.Г. Криминалистика: учебник. М.: Юрист, 2004. 639 с.
11. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Waltham, MA: Academic Press, 2011. 840 b.