“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=382

2026-yil
8-son
avgust
ISSN 3093-8546

Kibermakonda firibgarlikning oldini olishning tashkiliy-huquqiy mexanizmlari

Boburjon Suyunov,
Oʻzbekiston Respublikasi Kriminologiya tadqiqot instituti
mustaqil izlanuvchisi
e-mail: boburjonbaxadirovich1990@gmail.com

Аннотация. Maqolada kibermakonda sodir etiladigan firibgarlikning oldini olish tizimi tashkiliy va huquqiy jihatdan tahlil qilingan. Profilaktikaning toʻrt darajali – shaxsiy, platforma va telekommunikatsiya, bank-toʻlov hamda huquqni muhofaza qilish darajalaridagi tuzilishi asoslanib, har bir daraja uchun majburiyat va mas'uliyatning huquqiy mazmuni ochib berilgan. Oʻzbekiston Respublikasi qonunchiligini takomillashtirishga oid aniq takliflar shakllantirilgan.

Калит сўзлар. kiberfiribgarlik, profilaktika, “oq shovqin”, riskka asoslangan yondashuv, drop-hisob, toʻlov oluvchini tasdiqlash, raqamli platforma, huquqni muhofaza qilish organlari, kiberxavfsizlik strategiyasi.

Аннотация. В статье с организационно-правовой точки зрения проанализирована система предупреждения мошенничества, совершаемого в киберпространстве. Обоснована четырёхуровневая структура профилактики, включающая индивидуальный уровень, уровень цифровых платформ и телекоммуникаций, банковско-платёжный уровень, а также уровень правоохранительных органов. Раскрыто правовое содержание обязанностей и ответственности субъектов на каждом из указанных уровней. Сформулированы конкретные предложения по совершенствованию законодательства Республики Узбекистан.

Ключевые слова. кибермошенничество, профилактика, «белый шум», риск-ориентированный подход, дроп-счёт, подтверждение получателя платежа, цифровая платформа, правоохранительные органы, стратегия кибербезопасности.

Annotation. The article provides an organizational and legal analysis of the system for preventing fraud committed in cyberspace. It substantiates a four-tier prevention framework comprising the individual level, the digital platform and telecommunications level, the banking and payment level, and the law enforcement level. The legal content of the duties and responsibilities applicable at each level is examined. Specific proposals for improving the legislation of the Republic of Uzbekistan are formulated.

Keywords. cyber fraud, prevention, “white noise,” risk-based approach, mule account, confirmation of payee, digital platform, law enforcement agencies, cybersecurity strategy.

Raqamli xizmatlarning ommalashuvi jinoyatchilikning tarkibiy tuzilishini sezilarli darajada oʻzgartirdi. Ichki ishlar vazirligi eʼlon qilgan maʼlumotlarga koʻra, 2024-yilda mamlakatda roʻyxatga olingan jinoyatlarning 44,4 foizi kiberjinoyatlar hissasiga toʻgʻri kelgan, ularning qariyb 98 foizi bank kartalari bilan bogʻliq boʻlib, 2021–2024-yillarda fuqarolar va banklar 1,9 trln soʻmdan ortiq moddiy zarar koʻrgan [8]. 2026-yil yanvarida oʻtkazilgan yuqori darajadagi majlisda bu toifadagi jinoyatlarni fosh etish darajasining pastligi alohida tanqid qilindi [9]. Mazkur raqamlar nafaqat jinoyatchilikning miqdoriy oʻsishini, balki unga qarshi kurashning mavjud tashkiliy modelini qayta koʻrib chiqish zaruratini ham koʻrsatadi.

Kibermakonda sodir etiladigan firibgarlikning oʻziga xosligi shundaki, unda jinoyatchi bilan jabrlanuvchi oʻrtasida jismoniy aloqa boʻlmaydi, jinoyat hududiy chegara bilan bogʻlanmaydi, zarar esa bir necha daqiqa ichida bir nechta hisobraqamga tarqatilib yuboriladi. Shu sababli anʼanaviy profilaktika vositalari – profilaktik suhbat, ogohlantirish, profilaktik hisobga olish kabi “Huquqbuzarliklar profilaktikasi toʻgʻrisida”gi Qonunda [1] nazarda tutilgan choralarni raqamli muhitda bevosita qoʻllash qiyin. Amaliyotda bu boʻshliq ommaviy ogohlantirish, ijtimoiy reklama va “kartangiz kodini hech kimga aytmang” kabi xabarlar bilan toʻldirilmoqda.

Onlayn firibgarlikning oldini olish muammosi xorijiy kriminologiyada soʻnggi oʻn yil davomida mustaqil tadqiqot yoʻnalishiga aylandi. K. Kross va M. Kelli profilaktika tizimiga tanqidiy baho berib, ogohlantiruvchi xabarlarning haddan tashqari koʻpayishi ularning taʼsirini pasaytirishini, foydalanuvchi maʼlum vaqtdan keyin bunday xabarlarni bir-biridan ajratmay, umuman eʼtiborsiz qoldirishini “oq shovqin” muammosi sifatida taʼriflaydi [6]. Ushbu xulosa profilaktika samaradorligini oʻtkazilgan tadbirlar soni bilan emas, balki jabrlanish dinamikasi bilan oʻlchash zaruratini keltirib chiqaradi.

Oʻzbekistonlik tadqiqotchilar tomonidan ham kiberfiribgarlikning sabablari va sharoitlari, jabrlanuvchi bilan jinoyatchi oʻrtasidagi viktimologik munosabatni oʻrganish zarurligi qayd etilgan. Ayni paytda milliy adabiyotda profilaktikaning bank, telekom operatori va raqamli platforma majburiyatlari bilan bogʻliq tashkiliy-huquqiy jihatlari yetarlicha tadqiq etilmagan.

Kibermakonda firibgarlikning oldini olishning tashkiliy-huquqiy mexanizmi deganda, raqamli muhitda mulkiy aldov orqali sodir etiladigan jinoyatlarning sodir etilish imkoniyatini kamaytirishga qaratilgan normativ qoidalar, institutsional tuzilmalar, idoralararo axborot almashinuvi tartib-taomillari va subyektlar masʼuliyatining oʻzaro bogʻlangan tizimini tushunish lozim.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Shuningdek, mexanizmning ichki tuzilishini to‘rt darajaga ajratish maqsadga muvofiq. Birinchi – shaxsiy daraja bo‘lib, u raqamli va moliyaviy savodxonlikni oshirish, fishing xabarlari va soxta qo‘ng‘iroqlarni farqlash ko‘nikmasini shakllantirish, takroriy jabrlanishning oldini olish hamda keksalar, yoshlar va raqamli tajribasi kam shaxslar uchun maqsadli dasturlarni o‘z ichiga oladi. Ikkinchi – platforma va telekommunikatsiya darajasi: soxta akkauntlarni tezkor bloklash, telefon raqami va akkaunt obro‘sini tekshirish, shubhali ommaviy xabar tarqatishni aniqlash, qalbaki domenlarni cheklash hamda soxta raqamdan qo‘ng‘iroq qilish (spoofing) holatlarini aniqlash shu darajaga tegishli. Uchinchi – bank va to‘lov tashkilotlari darajasi, unda qabul qiluvchining ismini tasdiqlash, yangi ochilgan yoki xavf belgilariga ega hisoblarga o‘tkazmalarni qo‘shimcha tekshirish, qisqa vaqt ichida ko‘p hisobga tarqatilayotgan mablag‘larni aniqlash, drop-hisoblarni risk mezonlari asosida nazorat qilish va shubhali tranzaksiyani vaqtincha to‘xtatish choralari jamlanadi. To‘rtinchi – huquqni muhofaza qilish darajasi bo‘lib, u yagona kiberfiribgarlik ma'lumotlar bazasini yuritish, bank hisobi, telefon raqami, IP-manzil va akkauntlar bo‘yicha o‘zaro bog‘liqlikni aniqlash, seriyali jinoyatlarni birlashtirish, profilaktik hisob va risk xaritalarini yuritish hamda banklar, telekom operatorlari va raqamli platformalar bilan doimiy hamkorlikni nazarda tutadi.

Ushbu darajalar mustaqil emas, balki ketma-ket bog‘langan: birinchi darajada to‘xtatilmagan harakat ikkinchi darajada, u yerda ham to‘xtatilmasa — uchinchi darajada to‘siqqa uchrashi kerak. Mexanizmning samaradorligi eng kuchli bo‘g‘in bilan emas, eng zaif bo‘g‘in bilan belgilanadi, shu sababli har qanday darajadagi majburiyatning deklarativ qolishi butun tizimni ishdan chiqaradi.

Profilaktikaning amaldagi modelida yetakchi o‘rinni ommaviy ogohlantirish egallaydi. Biroq barcha shaxslarga bir xil mazmundagi xabarni uzluksiz yuborish ma'lum vaqtdan keyin teskari natija beradi. Kross va Kelli ta'kidlaganidek, ogohlantirishlar oqimi ortib borgan sari foydalanuvchi ular o‘rtasidagi farqni sezmay qo‘yadi va butun oqimni fon shovqini sifatida qabul qiladi [6]. Bunday holatda hatto o‘z vaqtida yuborilgan, aniq va to‘g‘ri xabar ham maqsadga yetib bormaydi.

Bu muammoning tashkiliy ildizi baholash mezonida yashiringan. Profilaktika faoliyati an'anaviy ravishda o‘tkazilgan tadbirlar, tarqatilgan xabarlar va qamrab olingan shaxslar soni bo‘yicha hisobga olinadi. Natijada tizim ko‘proq xabar tarqatishga rag‘batlantiriladi, holbuki maqsad jabrlanish holatlarini kamaytirish. Shu bois profilaktikaning hisobot ko‘rsatkichlarini qayta ko‘rib chiqish, ya'ni xabarlar soni o‘rniga muayyan toifadagi firibgarlikdan jabrlanish darajasining o‘zgarishi, takroriy jabrlanish ulushi va to‘xtatilgan o‘tkazmalar hajmi kabi natijaviy mezonlarga o‘tish zarur.

Firibgar odatda soxta qonuniylik belgilarini (rasmiy ramz, hujjat ko‘rinishi, “bank xizmati” nomidan qo‘ng‘iroq), vakolat va

shoshilinchlik taassurotini, kichik dastlabki foyda orqali ishonch hosil qilish usulini hamda uzoq muddatli emotsional aloqani birgalikda qoʻllaydi. Demak, ogohlantirish xabarida “ehtiyot boʻling” degan umumiy chaqiriq emas, aynan shu texnikalarni taniydigan belgilarni berish samaraliroq.

Ikkinchi muhim jihat – takroriy jabrlanish. Kross koʻrsatganidek, bir marta jabrlangan shaxs keyingi hujumlar uchun ustuvor nishonga aylanadi, chunki uning ma'lumotlari jinoiy guruhlar oʻrtasida aylanma savdo predmetiga aylanadi [7]. Bu holat profilaktikada uchlamchi darajani, ya'ni allaqachon jabrlangan shaxslar bilan individual ishlashni mustaqil yoʻnalish sifatida ajratishni talab qiladi. Amalda buning tashkiliy shakli ariza qabul qilingan paytdan boshlab jabrlanuvchini profilaktik kuzatuvga olish, uning hisoblari boʻyicha kuchaytirilgan monitoring rejimini joriy etish va takroriy murojaat holatlarini alohida hisobga olishdan iborat boʻlishi mumkin.

Kibermakonda firibgarlik faqat jabrlanuvchining xatosi orqali emas, balki muayyan xizmatlar: hisob ochish, raqam ajratish, domen roʻyxatdan oʻtkazish, oʻtkazmani amalga oshirish yordamida sodir etiladi. Shu bois bu xizmatlarni koʻrsatuvchi subyektlarga nisbatan aniq majburiyatlar belgilanishi profilaktikaning huquqiy oʻzagini tashkil etadi.

Moliyaviy sohada xalqaro standartlar soʻnggi yillarda sezilarli oʻzgardi. FATF 2026-yil fevralida e'lon qilgan hujjatda kibermakonda sodir etiladigan firibgarlik eng keng tarqalgan va eng katta noqonuniy daromad keltiruvchi jinoyat turlaridan biri sifatida baholanib, unga qarshi kurashda FATF standartlarining toʻrt yoʻnalishi ajratilgan: toʻlovlarning shaffofligini oshirish va qabul qiluvchini tasdiqlash (confirmation of payee) mexanizmlarini joriy etish; aktivlarni qaytarish doirasida toʻlovni toʻxtatib turish va muzlatish vositalari hamda aybdorlikni aniqlamasdan musodara imkoniyati; virtual aktivlarni tartibga solish; xalqaro hamkorlik va axborot almashinuvini tezlashtirish [10]. 2025-yil iyunida qabul qilingan 16-tavsiyaning yangi tahriri esa toʻlov xabarlarida joʻnatuvchi va oluvchi toʻgʻrisidagi ma'lumotlar tarkibini birxillashtirishni va firibgarlikdan himoya vositalarini joriy etishni talab qiladi [11].

Mamlakatimizda bu yoʻnalishda dastlabki qadamlar qoʻyilgan. Prezidentning 2025-yil 30-apreldagi PQ-153-son qarori bilan banklar va toʻlov tashkilotlarining axborot xavfsizligi talablariga rioya etish borasidagi mas'uliyatini kuchaytirish, tizimida eng koʻp kiberjinoyat qayd etilgan tashkilotlar roʻyxatini har oyda ommaga e'lon qilish, Markaziy bank tomonidan tranzaksiyalarni monitoring qilish orqali firibgarlik sxemalari belgilarini aniqlash va huquqni muhofaza qiluvchi organlarga tezkor xabar berish tizimini yoʻlga qoʻyish, shuningdek jinoyat sodir etishda axborot texnologiyalaridan foydalanishni javobgarlikni ogʻirlashtiruvchi holat sifatida belgilash vazifalari nazarda tutilgan [4]. Shu qarorda huquqni muhofaza qiluvchi organlarning bank siriga oid soʻrovlari ijrosining aniq

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

muddatlarini belgilash talabi ham mustahkamlangan – bu tezkorlik masalasida prinsipial ahamiyatga ega, zero firibgarlik natijasida oʻtkazilgan mablagʻ koʻp hollarda bir soat ichida bir nechta hisobga tarqatib yuboriladi.

Platforma va telekom operatorlari darajasida esa tartibga solish nisbatan zaif qolmoqda. Amalda soxta akkauntni bloklash, qalbaki domenni oʻchirish yoki spoofing qoʻngʻirogʻini toʻxtatish muddatlarining belgilanmaganida, shuningdek murojaatga javob bermaslik uchun javobgarlik nazarda tutilmaganida koʻrinadi. “Kiberxavfsizlik toʻgʻrisida”gi Qonun [2] va unga bogʻliq oʻzgartirishlar [3] kiberxavfsizlik subyektlarining umumiy majburiyatlarini belgilaydi, biroq firibgarlikka qarshi aniq operatsion talablar — javob chorasi muddati, soxta raqamni filtrlash, ommaviy xabar tarqatishni cheklash normativ darajada batafsillashtirilishi zarur.

Huquqni muhofaza qilish darajasida 2026-yil 10-martdagi PF-38-son Farmon bilan tasdiqlangan 2026–2030-yillarga moʻljallangan Kiberxavfsizlik strategiyasi muhim burilish nuqtasi boʻldi. Unda kiberjinoyatchilikka faol qarshi kurashish, raqamli kriminalistika imkoniyatlarini va ixtisoslashtirilgan boʻlinmalar salohiyatini oshirish, kibermakondagi firibgarliklarning oldini olish va fuqarolarni xabardor qilib borish, kiberjinoyatlar boʻyicha ariza va xabarlarni topshirish jarayonini onlayn-xizmatlar va maxsus platformalar orqali soddalashtirish vazifalari belgilangan [5]. Strategiyaning profilaktika nuqtayi nazaridan eng qimmatli jihati shundaki, u oldini olishni faqat targʻibot sifatida emas, huquqni muhofaza qilish organining mustaqil vazifasi sifatida qayd etadi.

Yuqorida bayon etilgan tahlil profilaktikaning yangi maqsadli raqamli profilaktikani taklif etish imkonini beradi.

Maqsadli raqamli profilaktika – shaxs, tranzaksiya, bank hisobi, akkaunt, telefon raqami yoki raqamli xatti-harakatning risk darajasiga qarab avtomatlashtirilgan va individuallashtirilgan profilaktik choralarni qoʻllashga qaratilgan faoliyatdir. Uning umumiy profilaktikadan farqi shundaki, chora barcha shaxslarga bir xilda emas, balki aniqlangan riskka javoban qoʻllaniladi.

Oʻtkazilgan tahlil kibermakonda firibgarlikning oldini olish samaradorligi birinchi navbatda ogohlantirish hajmiga emas, balki xizmat koʻrsatuvchi subyektlar majburiyatining aniqligiga va darajalararo axborot almashinuvining tezligiga bogʻliq ekanini koʻrsatdi. Shu asosda quyidagi takliflar ilgari suriladi.

Birinchidan, “Huquqbuzarliklar profilaktikasi toʻgʻrisida”gi Qonunni raqamli muhitda profilaktika choralarini qoʻllashga bagʻishlangan alohida bob (modda) bilan toʻldirish, unda maqsadli raqamli profilaktika tushunchasi, uning subyektlari, asoslari va protsessual kafolatlarini mustahkamlash maqsadga muvofiq.

Ikkinchidan, qonunchilikda “kiberfiribgarlik” va “drop-hisob” tushunchalarining huquqiy taʼrifini belgilash, shuningdek oʻz nomidagi bank kartasi, hisobraqami yoki SIM-kartasini boshqa shaxsga jinoiy maqsadda foydalanish uchun berish uchun

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

javobgarlik normasini aniqlashtirish talab etiladi.

Uchinchidan, to‘lovlarda qabul qiluvchining ma'lumotlarini tasdiqlash (confirmation of payee) mexanizmini bosqichma-bosqich majburiy joriy etish, bu FATFning 16-tavsiyasi yangi tahriri talablariga muvofiqdir.

To‘rtinchidan, shubhali o‘tkazmani qisqa va aniq belgilangan muddatga vaqtincha to‘xtatib turish institutini — uni qo‘llash asoslari, muddati, xabardor qilish tartibi va shikoyat qilish mexanizmi bilan birgalikda qonun darajasida mustahkamlash zarur.

Beshinchidan, Ichki ishlar vazirligi, Markaziy bank, Kiberxavfsizlik markazi, telekom operatorlari va raqamli platformalarning o‘zaro bog‘langan yagona kiberfiribgarlik ma'lumotlar bazasini tashkil etish, uning huquqiy maqomi, ma'lumot tarkibi va foydalanish tartibini normativ hujjat bilan belgilash taklif etiladi.

Ushbu takliflarning amalga oshirilishi profilaktikani ommaviy ogohlantirish darajasidan aniq majburiyat, aniq muddat va aniq javobgarlikka asoslangan huquqiy institut darajasiga ko‘tarish imkonini beradi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining 2014-yil 14-maydagi O‘RQ-371-son “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi Qonuni // Qonun hujjatlari ma'lumotlari milliy bazasi.

2. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni // Qonun hujjatlari ma'lumotlari milliy bazasi.

3. O‘zbekiston Respublikasining 2024-yil 20-sentyabrdagi O‘RQ-964-son “Kiberxavfsizlikni ta'minlash sohasidagi qonunchilik takomillashtirilishi munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi Qonuni.

4. O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-son “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi Qarori.

5. O‘zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi PF-38-son “O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida”gi Farmoni.

6. Cross C., Kelly M. The problem of “white noise”: examining current prevention approaches to online fraud // Journal of Financial Crime. 2016. Vol. 23, № 4. – P. 806–828.

7. Cross C. Using financial intelligence to target online fraud victimisation: applying a tertiary prevention perspective // Criminal Justice Studies. 2016. – Vol. 29, № 2. – P. 124–145.

8. O‘zbekistonda 2021–2024-yillarda banklar va fuqarolar kiberjinoyatlardan 1,9 trln so‘m zarar ko‘rdi // Gazeta.uz. 2025-yil 29-may.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

9. Prezident IIVning kiberjinoyatchilikka qarshi kurashish bo‘yicha faoliyatini tanqid qildi // Gazeta.uz. – 2026-yil 27-yanvar.

10. FATF. Illicit Financial Flows from Cyber-enabled Fraud. Paris: FATF, February 2026. –

11. FATF. Updated Standards on Recommendation 16 (Payment Transparency). Paris: FATF, June 2025. – www.fatf-gafi.org.