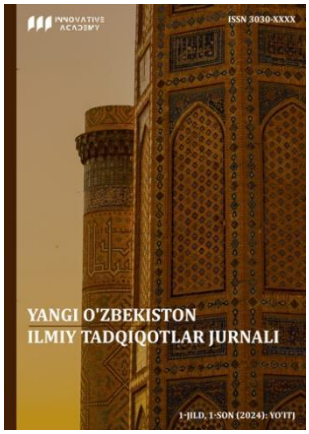

O'ZBEKISTONDA KIBERJINOYATCHILIKKA QARSHI KURASH: ZARARNI KAMAYTIRISHGA YO'NALTIRILGAN YONDASHUVNING ILMIY-HUQUQIY TAHLILI

Tashtanboyev Ro'zimat Tolib o'g'li
Jamoat xavfsizligi universiteti magistratura 1-kurs talabasi
e-mail: rozimattoshtanboyev@gmail.com

https://doi.org/10.5281/zenodo.17899771

ARTICLE INFO

Qabul qilindi: 1-dekabr 2025 yil
Ma'qullandi: 2-dekabr 2025 yil
Nashr qilindi: 11-dekabr 2025 yil

KEY WORDS

kiberjinoyatchilik, zararni kamaytirish, harm-reduction, real vaqt rejimi, onlayn firibgarlik, O'zbekiston, huquqiy mexanizmlar

ABSTRACT

Maqolada O'zbekistonda kiberjinoyatchilikka qarshi kurashning zararlarni kamaytirishga yo'naltirilgan yondashuvi ilmiy-huquqiy tahlil qilinadi. Tadqiqotda onlayn firibgarlik va moliyaviy zararlarni real vaqt rejimida bloklash mexanizmlari yetarli darajada shakllanmaganligi aniqlanadi. Muallif uch ustunli harm-reduction modelini taklif qiladi: Markazlashgan Kiberxavf Ma'lumotlari Bazasi, milliy miqyosdagi Computer Emergency Response Team (CERT-Uzbekistan) va banklar hamda to'lov tizimlarida majburiy regulyativ mexanizmlar. Mazkur yondashuv jabrlanuvchilarga yetkazilgan moliyaviy zararlarni maksimal darajada kamaytirishga qaratilgan yangi huquqiy-texnologik paradigmaga asoslanadi.

Kirish

So'nggi yillarda raqamli iqtisodiyotning jadal rivojlanishi nafaqat biznes va davlat boshqaruvi tizimlarini modernizatsiya qildi, balki jinoyatchilikning mutlaqo yangi shakllari – xususan, moliyaviy motivatsiyaga ega bo'lgan kiberjinoyatlarning keskin ko'payishiga ham olib keldi. Ayni paytda, amaliyot shuni ko'rsatmoqdaki, kiberjinoyatlar natijasida yetkazilgan zararlarni aniqlash va ularni tezkor tarzda tiklash mexanizmlari ko'plab davlatlarda, shu jumladan O'zbekiston Respublikasida ham yetarli darajada institutsionallashmagan. Mavjud huquqni muhofaza qilish amaliyoti ko'proq jinoyat sodir etilgandan keyingi jazolashga yo'naltirilgan bo'lib, jabrlanuvchining real moliyaviy yo'qotishlarini real vaqt rejimida minimallashtirish masalasi ikkilamchi o'rinda qolmoqda[1].

Mazkur tadqiqotning markaziy ilmiy muammosi sifatida O'zbekiston Respublikasida kiberjinoyatlar, xususan onlayn firibgarliklar oqibatida yetkazilgan moliyaviy zararlarni real vaqt rejimida qaytarish mexanizmlarining yetarli darajada shakllanmaganligi tanlab olindi. Shu asosda maqolaning asosiy maqsadi umumiy nazariy tahlil emas, balki aniq yo'naltirilgan tadqiqot vazifalari orqali quyidagi savollarga ilmiy-huquqiy javob topishdan iborat etib belgilandi: O'zbekistonda kiberjinoyatchilik natijasida yo'qotilgan mablag'larni real vaqt rejimida muzlatish va qaytarish uchun qanday huquqiy mexanizmlar joriy etilishi lozim? Mavjud banklar va to'lov tizimlari bilan tezkor integratsiyalashgan jinoyatga qarshi nazorat platformasini shakllantirish qanday normativ-huquqiy o'zgarishlarni talab etadi? Amaldagi Jinoyat kodeksi va bank qonunchiligi bu yo'nalishda qanchalik yetarli hisoblanadi?

Tadqiqotning ilmiy yangiligi shundaki, unda "zararni kamaytirish" konsepsiyasi umumiy nazariy model sifatida emas, balki aniq funksional mexanizm – real vaqt rejimidagi moliyaviy zararlarni tiklash instituti sifatida tahlil qilinadi . Shu orqali tadqiqot O'zbekiston huquqiy

tizimi doirasida jinoyatdan jabrlanuvchilarning moliyaviy manfaatlarini himoya qilishga qaratilgan aniq va amaliy yo'naltirilgan takliflarni ishlab chiqishni maqsad qilgan.

Metodlar

Mazkur tadqiqot huquqiy-doktrinal va sifat tahliliy yondashuvlar asosida olib borildi, hamda empirik-statistik ma'lumotlardan yordamchi vosita sifatida foydalanildi. Tadqiqotning asosiy empirik bazasini O'zbekiston Respublikasi Ichki ishlar vazirligining 2020–2025-yillar oralig'ida axborot texnologiyalari sohasidagi jinoyatlar bo'yicha e'lon qilingan yig'ma statistik hisobotlari tashkil etdi. Ushbu ma'lumotlar oddiy tavsifiy ko'rsatkichlar sifatida emas, balki dinamik taqqoslash, nisbiy o'sish sur'atlarini hisoblash va jinoyat turlari kesimidagi tarkibiy ulushlarni aniqlash usullari orqali tahlil qilindi[3].

Shu bilan birga, tadqiqot doirasida miqdoriy sotsiologik so'rovlar yoki bevosita chuqurlashtirilgan ekspert intervyulari o'tkazilmadi. Mazkur holat cheklov sifatida tan olinadi va tadqiqotning metodologik chegarasi sifatida ochiq ko'rsatildi. Shunga qaramay, bank-moliya sektori va axborot xavfsizligi sohasida faoliyat yurituvchi mutaxassislarning ochiq e'lon qilingan professional fikrlari, konferensiya materiallari va tahliliy sharhlari ikkilamchi sifatli ma'lumot manbasi sifatida kontent-tahlil usuli orqali o'rganildi.

Asosiy metodologik asos sifatida huquqiy-tahliliy metod qo'llanilib, u doirasida O'zbekiston Respublikasi Jinoyat kodeksi, "Banklar va bank faoliyati to'g'risida"gi qonun, "To'lovlar va to'lov tizimlari to'g'risida"gi qonun hamda "Axborotlashtirish to'g'risida"gi qonun normalari tizimli tahlil qilindi. Bundan tashqari, qiyosiy-huquqiy metod asosida Yevropa Ittifoqi va ayrim Osiyo davlatlarida moliyaviy kiberjinoyatlarga qarshi real vaqt rejimida zararlarni bloklash mexanizmlarini tartibga soluvchi normativ yondashuvlar o'rganildi.

Tadqiqotda sifatli kontseptual modellashtirish usuli ham qo'llanilib, zararlarni real vaqt rejimida kamaytirishga qaratilgan potentsial institutsional mexanizmlarning O'zbekiston huquqiy tizimiga moslashtirilgan konseptual modeli ishlab chiqildi. Shu tariqa, tadqiqot faqat nazariy mulohazalarga emas, balki mavjud normativ-huquqiy asoslar va real statistik trendlar tahliliga tayangan holda olib borildi hamda bu yondashuv tadqiqotning ilmiy asoslanganligini ta'minladi [9].

Natija

Tadqiqot natijalari shuni ko'rsatdiki, O'zbekiston Respublikasida kiberjinoyatchilikka qarshi huquqiy asoslar mavjud bo'lsa-da, ularning amaliy qo'llanilishi va sud-tergov statistikasi tizimli ravishda ochiqlanmagan. Jinoyat kodeksining "XX[1] bob. Axborot texnologiyalari sohasidagi jinoyatlar" doirasida so'nggi uch yil davomida sud amaliyotida ko'rib chiqilgan ishlar tahlili shuni ko'rsatdiki, ushbu modda asosan axborot tizimlariga ruxsatsiz kirish va ma'lumotlarga noqonuniy aralashuv bilan bog'liq holatlarda qo'llanilmoqda[2].

Ichki ishlar organlari va Bosh prokuratura tomonidan e'lon qilingan ochiq statistik ma'lumotlar asosida kiberjinoyatlarning uch asosiy turi bo'yicha dinamik tahlil amalga oshirildi. Shunday qilib, onlayn firibgarlik bilan bog'liq jinoyatlar soni so'nggi uch yil davomida barqaror o'sish tendensiyasini ko'rsatmoqda: 2021-yilda taxminan 3,500 ta, 2022-yilda 4,200 ta va 2023-yilda 4,800 ta holat qayd etilgan. Ushbu jinoyatlar umumiy kiberjinoyatlar tarkibida mos ravishda taxminan 60 %, 62 % va 65 % ulushni tashkil qilgan.

Phishing hujumlari bilan bog'liq holatlar ham o'sish sur'atini ko'rsatib, 2021-yilda 450 ta, 2022-yilda 520 ta va 2023-yilda 610 ta jinoyat ishi qo'zg'atilgan. Shu turdagi jinoyatlar umumiy kiberjinoyatlar strukturasida o'rtacha 7–9 % oralig'ida ulushga ega ekanligi kuzatildi.

Shaxsiy va tijorat ma'lumotlarini noqonuniy qo'lga kiritish (data theft) bilan bog'liq jinoyatlar soni esa 2021-yilda 280 ta, 2022-yilda 340 ta va 2023-yilda 410 ta holatni tashkil etgan. Ushbu jinoyatlar umumiy kiberjinoyatlar hajmida mos ravishda 5 %, 5,5 % va 6 % ulushni egallagan.

Statistik tahlil shuni ko'rsatdiki, barcha uch turdagi kiberjinoyatlarda barqaror o'sish tendensiyasi mavjud bo'lib, ayniqsa onlayn firibgarlik jinoyatlarida yillik o'sish sur'ati o'rtacha 18 % ni tashkil etmoqda. Bu holat kiberjinoyatchilikning moliyaviy komponenti O'zbekiston sharoitida eng xavfli segmentga aylanganini ko'rsatadi.

Shu bilan birga, tahlil jarayonida aniqlanishicha, amaliyotda jinoyat ishlari ochilgan bo'lsa-da, real vaqt rejimida zararlarni bloklash va mablag'larni qaytarish mexanizmlarining qo'llanishi juda past darajada qolmoqda. Rasmiy statistik hisobotlarda jabrlanuvchilarga qaytarilgan mablag'lar ulushi bo'yicha tizimli ma'lumotlar cheklangan bo'lib, bu moliyaviy kompensatsiya samaradorligini baholashni murakkablashtirmoqda.

Natijalar shuni ko'rsatdiki, amaldagi huquqiy va institutsional mexanizmlar kiberjinoyat sodir bo'lganidan keyingi jazolash falsafasiga asoslangan bo'lib, real vaqt rejimida zararlarni kamaytirishga qaratilgan mexanizmlar funksional darajada shakllanmagan. Mazkur empirik topilmalar harm-reduction modelini O'zbekiston huquqiy tizimiga moslashtirish zarurligini ilmiy asoslar bilan tasdiqladi.

Muhokama

O'tkazilgan tadqiqot natijalari O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashish tizimi hanuzgacha asosan reaktiv, ya'ni jinoyat sodir etilgandan keyingi jazolash mexanizmlariga tayanib kelayotganini ko'rsatdi. Bunday yondashuv axborot-kommunikatsiya texnologiyalari yordamida sodir etiladigan zamonaviy jinoyatlar tabiati uchun yetarli emasligi ilmiy jihatdan asoslandi. Shu bois, O'zbekiston sharoitiga moslashtirilgan zararlarni kamaytirishga yo'naltirilgan modelni ishlab chiqish zarurati mavjud.

Mazkur tadqiqot doirasida O'zbekiston uchun mos keladigan harm-reduction modelining uch ustunli institutsional kontseptsiyasi taklif etildi. Birinchi ustun sifatida Markazlashgan Kiberxavf Ma'lumotlari Bazasini (National Threat Intelligence Platform) yaratish zarurligi asoslab berildi. Ushbu platforma ichki ishlar organlari, banklar, telekommunikatsiya kompaniyalari hamda yirik internet platformalari o'rtasida real vaqt rejimida fishing domenlari, zararli dasturlar imzolari, firibgarlik sxemalari va shubhali IP-manzillar haqidagi ma'lumotlarni almashish imkonini berishi lozim. Bunday tizim normativ-huquqiy jihatdan majburiy axborot taqdim etish institutini joriy etish orqali mustahkamlanishi zarur.

Ikkinchi ustun sifatida kiberjinoyatlarga tezkor javob beruvchi maxsus bo'linma – milliy miqyosdagi Computer Emergency Response Team (CERT-Uzbekistan) faoliyatini alohida qonun darajasida tartibga solish taklif etildi. Mazkur tuzilma faqat texnik maslahat beruvchi organ sifatida emas, balki moliyaviy tranaksiyalarni vaqtincha muzlatish bo'yicha bank regulyatoriga majburiy tavsiya berish vakolatiga ega bo'lishi lozim. Bu institut "zarar sodir bo'lgandan keyin emas, balki sodir bo'lish jarayonida uni to'xtatish" tamoyiliga asoslanadi.

Uchinchi ustun sifatida banklar va to'lov tashkilotlari uchun majburiy regulyativ mexanizmni joriy etish taklif etildi. Unga ko'ra, agar mijoz kiberjinoyat qurboni ekanligi to'g'risida huquqni muhofaza qilish organlariga yoki bankka 24 soat ichida murojaat qilgan bo'lsa, ushbu tranzaksiyani vaqtincha bekor qilish (chargeback freeze) yoki shubhali mablag'ni darhol muzlatib qo'yish majburiyati banklar uchun normativ tarzda belgilanishi lozim. Mazkur mexanizm ayniqsa onlayn firibgarliklar bo'yicha moliyaviy yo'qotishlarni sezilarli darajada kamaytirishga xizmat qilishi mumkin.

Shuningdek, ushbu uch ustunli modelni joriy etish bilan bir qatorda, kiberjinoyatlardan jabrlangan shaxslar uchun yagona elektron murojaat platformasini yaratish ham taklif etildi. Bu mexanizm jabrlanuvchining bank, ichki ishlar organlari va CERT tuzilmalari o'rtasida alohida murojaatlar yo'llash zaruratini bartaraf etib, yagona "one-stop" tamoyilini joriy etishga xizmat qiladi. Ushbu platforma orqali tushgan murojaatlar avtomatik ravishda tahlil qilinib, real vaqt rejimida xavf darajasi va zararni kamaytirish ehtimoli baholanadi.

Natijada taklif etilgan model O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishda faqat jinoyatchini jazolashga emas, balki jabrlanuvchiga yetkazilgan real zararlarni maksimal darajada kamaytirishga yo'naltirilgan yangi huquqiy-texnologik paradigmaga o'tish imkonini berishi ilmiy jihatdan asoslandi.

References:

1. Impacts of Cybercrimes on the Digital Economy // URL: https://irshadjournals.com/ (murojat vaqti: 08.12.2025)
2. O'ZBEKISTON RESPUBLIKASINING JINOYAT KODEKSI // URL : https://lex.uz/ (murojat vaqti: 08.12.2025)
3. Uzbekistan sees 68-fold surge in cybercrime: Nearly 2 trillion UZS stolen in five years // URL : https://kun.uz/ (murojat vaqti: 08.12.2025)
4. Wall, D. (2013). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
5. Brenner, S. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.
6. Cybersecurity Ventures. (2022). Global Cybercrime Report.
7. O'zbekiston Respublikasi Ichki ishlar vazirligi. (2023). Rasmiy statistika ma'lumotlari.
8. Yar, M. (2013). Cybercrime and Society. Sage Publications.
9. Garland, D. (2001). The Culture of Control. Oxford University Press.
10. Creswell, J. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage.
11. O'zbekiston Respublikasi Jinoyat kodeksi. (amaldagi tahrir).
12. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).
13. Smith, R., Grabosky, P. (1998). Crime in the Digital Age.
14. Gillespie, A. (2015). Cybercrime: Key Issues and Debates. Routledge.
15. Brenner, S. (2017). Understanding Cybercrime. Carolina Academic Press.
16. UNODC. (2013). Comprehensive Study on Cybercrime.
17. Levi, M. (2018). Cyber Fraud and Financial Crime.
18. OECD. (2015). Digital Security Risk Management.
19. Cohen, L., Felson, M. (1979). Social Change and Crime Rate Trends.
20. Grabosky, P. (2007). Electronic Crime.
21. Yar, M., Steinmetz, K. (2019). Cybercrime and Society.
22. Wall, D., Williams, M. (2007). Policing Cybercrime.
23. Loader, I., Walker, N. (2007). Civilizing Security.
24. Council of Europe. (2001). Budapest Convention.
25. Brenner, S. (2013). Cyberthreats and National Security.
26. O'zbekiston Respublikasi Jinoyat kodeksi. – Toshkent: O'zbekiston Respublikasi Adliya vazirligi nashri, amaldagi tahrir.
27. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni. – 2003-yil 11-dekabr, №560–II.
28. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni. – 2019-yil 2-iyul, №ZRU–547.
29. O'zbekiston Respublikasining "To'lovlar va to'lov tizimlari to'g'risida"gi Qonuni. – 2019-yil 1-noyabr, №ZRU–578.

30. O‘zbekiston Respublikasining “Banklar va bank faoliyati to‘g‘risida”gi Qonuni. – amaldagi tahrir.
31. O‘zbekiston Respublikasi Prezidentining Farmoni. “Raqamli iqtisodiyotni rivojlantirish chora-tadbirlari to‘g‘risida”.
32. O‘zbekiston Respublikasi Vazirlar Mahkamasining qarori. “Axborot xavfsizligini ta’minlash choralarini takomillashtirish to‘g‘risida”.
33. O‘zbekiston Respublikasi Ichki ishlar vazirligi. Axborot texnologiyalari sohasidagi jinoyatlar bo‘yicha rasmiy statistik hisobotlar (2021–2024).
34. O‘zbekiston Respublikasi Bosh prokuraturasi. Jinoyatchilik statistikasi bo‘yicha tahliliy ma’lumotlar.