VOLUME-4, ISSUE-05

"KIBERFIRGARLIKNING JINOIY-HUQUQIY TAVSIFI"

Muxammadiyeva Sevara Yolg‘oshovna
Surxondaryo viloyati Termiz davlat
universiteti Yuridik fakulteti
Yurisprudensiya yo’nalishi talabasi

Annotatsiya: Ushbu maqolada kiberfirgarlik jinoyatining jinoiy-huquqiy tavsifi, uning obyekti, obyektiv tomoni, subyekti va subyektiv tomoni kabi tarkibiy elementlari ilmiy-nazariy jihatdan tahlil qilingan. Axborot texnologiyalari rivojlanishi natijasida kiberfirgarlikning an’anaviy firgarlikdan farqli xususiyatlari, xususan, jinoyat predmeti sifatida raqamli aktivlar va elektron ma’lumotlarning o‘rni yoritilgan. Shuningdek, milliy qonunchilikdagi bo‘shliqlar va ularni xalqaro andozalar asosida takomillashtirish bo‘yicha takliflar ilgari surilgan.

Kalit so‘zlar: kiberfirgarlik, kiberjinoyatchilik, obyekt, obyektiv tomon, raqamli aktivlar, kvalifikatsiya, fshing, kiberxavfsizlik, elektron dalillar.

Abstract: This article provides a scientific and theoretical analysis of the criminal-legal characteristics of cyber fraud, exploring its constituent elements: the object, objective side, subject, and subjective side. In light of the rapid advancement of information technologies, the distinctive features of cyber fraud compared to traditional fraud are highlighted, with a specific focus on digital assets and electronic data as the objects of the crime. Furthermore, gaps in national legislation are identified, and recommendations are put forward for legal improvement based on international standards.

Keywords: cyber fraud, cybercrime, object, objective side, digital assets, qualification, phishing, cybersecurity, electronic evidence.

Kirish

Global raqamlashtirish va axborot-kommunikatsiya texnologiyalarining (AKT) hayotimizga shiddat bilan kirib borishi nafaqat iqtisodiy o‘sishni ta’minladi, balki jinoiy dunyoning ham transformatsiyalashuviga olib keldi. Bugungi kunda an’anaviy jinoyat turlari virtual makonga ko‘chib, yangi shakl va usullarda namoyon bo‘lmoqda. Bular orasida eng xavflisi va keng tarqalayotgani kiberfirgarlik (cyber fraud) hisoblanadi.

Kiberfirgarlik nafaqat alohida fuqarolarning moddiy mablag‘lariga, balki yirik korxonalar, moliya institutlari va davlatning iqtisodiy xavfsizligiga ham jiddiy tahdid solmoqda. Jinoyatchilarning transchegaraviy tabiati, anonimlikni saqlash imkoniyatlari va ilg‘or algoritmlardan (masalan, sun’iy intellekt, fshing va ijtimoiy muhandislik) foydalanishi ushbu qilmishlarni fosh etish va huquqiy baho berishni murakkablashtiradi. Ushbu maqolaning maqsadi kiberfirgarlikning jinoiy-huquqiy tabiatini fundamental tahlil qilish, uni sodir etish mexanizmlarini o‘rganish hamda O‘zbekiston Respublikasi Jinoyat kodeksi va xalqaro tajriba doirasida ushbu jinoyat turiga to‘g‘ri jinoiy-huquqiy tavsif (kvalifikatsiya) berish muammolarini yoritishdan iborat.

Asosiy Qism: Kiberfirgarlikning Jinoiy-Huquqiy Tarkibi

Kiberfirgarlikni to‘g‘ri kvalifikatsiya qilish uchun uning jinoiy-huquqiy tarkibini (korpus delicti) tashkil etuvchi to‘rtta elementni aniq belgilab olish lozim.

2.1. Jinoyatning Obyekti va Predmeti

Har qanday firgarlik kabi, kiberfirgarlikning ham umumiy obyekti mulkiy munosabatlardir. Biroq uning bevosita obyekti axborot tizimlari va telekommunikatsiya tarmoqlaridan foydalangan holda mulkka egalik qilish, undan foydalanish va uni tasarruf etish borasidagi ijtimoiy munosabatlar hisoblanadi.

Bu yerda jinoyat predmetiga alohida to‘xtalish lozim:

An’anaviy firgarlikda predmeti: Naqd pul, moddiy ashyolar yoki mulkka bo‘lgan huquqni tasdiqlovchi hujjatlar.

Kiberfirgarlikda predmeti: Elektron pullar, kriptovalyutalar, bank hisobraqamlaridagi raqamli mablag‘lar, shuningdek, shaxsiy ma’lumotlar (login, parol, plastik karta pin-kodlari) — bular moddiy bo‘lmagan, lekin iqtisodiy qiymatga ega bo‘lgan “raqamli aktivlar”dir.

2.2. Jinoyatning Obyektiv Tomoni

Kiberfirgarlikning obyektiv tomoni subyektning AKT vositalaridan foydalanib, o‘zganing mulkini yoki mulkka bo‘lgan huquqini aldash yoki ishonchni suiiste’mol qilish yo‘li bilan qonunga xilof ravishda o‘zlashtirishi bilan tavsiflanadi.

Bugungi kunda obyektiv tomondan kiberfirgarlik quyidagi usullarda namoyon bo‘lmoqda:

Fshing (Phishing): Soxta veb-saytlar yoki elektron xatlar orqali foydalanuvchilarning maxfiy ma’lumotlarini qo‘lga kiritish.

Ijtimoiy muhandislik (Social Engineering): Psixologik manipulyatsiya orqali jabrlanuvchini o‘z ixtiyori bilan pul o‘tkazishga majbur qilish.

Zararli dasturlar (Malware): Bank ilovalari yoki tizimlariga viruslar yuborib, tranzaksiyalarni yashirincha boshqarish.

Nazariy muammo: An'anaviy firgarlikda aldash *shaxsga* qaratilgan bo'ladi. Kiberfirgarlikda esa jinoyatchi ko'pincha insonni emas, balki *kompyuter tizimini (avtomatlashtirilgan dasturni)* aldaydi (masalan, soxta algoritm kiritish orqali). Ko'plab huquqshunos olimlarning fikricha, kompyuter tizimini "aldash" tushunchasi klassik firgarlik doirasiga tushmaydi va bu qilmishni kompyuter tizimlariga ruxsatsiz kirish jinoyatlari bilan komulyativ (birgalikda) kvalifikatsiya qilishni talab etadi.

2.3. Jinoyatning Subyekti va Subyektiv Tomoni

Jinoyat subyekti: Jinoyat qonunchiligiga ko'ra aqli raso, jinoiy javobgarlik yoshiga (O'zbekistonda 16 yoshga) to'lgan jismoniy shaxs. Zamonaviy kiberfirgarlik ko'pincha individual emas, balki yuqori texnologik bilimlarga ega bo'lgan uyushgan jinoiy guruhlar (hakerlar) tomonidan sodir etilishi bilan ajralib turadi.

Subyektiv tomoni: Faqatgina to'g'ridan-to'g'ri qasd va g'arazli maqsad bilan tavsiflanadi. Jinoyatchi o'z harakatlarining ijtimoiy xavfliligini anglaydi, moddiy zarar yetkazilishini ko'zlaydi va buni amalga oshirishni xohlaydi.

3. Qonunchilik Tahlili va Xalqaro Tajriba

O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasi (Firgarlik) 2016-yildagi o'zgarishlardan so'ng "kompyuter texnikasi vositalaridan foydalanib" sodir etilganlik uchun maxsus kvalifikatsiya belgilari (168-modda, 3-qism, "g" bandi) bilan to'ldirildi. Biroq, qonunchilikda hali ham bir qator muammolar mavjud:

Kriptovalyutalar maqomi: Kriptovalyutalar (Bitcoin, USDT va h.k.) o'g'irlangan holatlarda jinoyat predmetini mulk sifatida baholashda huquqni muhofaza qiluvchi organlar orasida yagona amaliyot shakllanmagan.

Transchegaraviylik: Jinoyatchi bir davlatda (masalan, Rossiyada) o'tirib, serverni boshqa davlatda (masalan, AQShda) joylashtirib, O'zbekiston fuqarosini chuv tushirsa, yurisdiksiya masalasini hal etish murakkablashadi. Kiberjinoyatchilik to'g'risidagi Budapesht konvensiyasi (2001) normalariga ko'ra, kiberfirgarlik (Computer-related fraud) har qanday kompyuter ma'lumotlarini kiritish, o'zgartirish, o'chirish yoki yo'q qilish orqali boshqa shaxsga iqtisodiy zarar yetkazgan holda qonuniy asoslarsiz mulkiy foyda ko'rish deb belgilangan. Bizning milliy qonunchilikni ham ushbu kengaytirilgan ta'rifga moslash lozim.

Xulosa

Kiberfirgarlikning jinoiy-huquqiy tavsifi huquqshunoslik fanidan zamonaviy texnologik realliklarni hisobga olishni talab etadi. O'tkazilgan ilmiy tahlil asosida quyidagi xulosalarga

kelindi:

Qonunchilikni unifikatsiya qilish: Jinoyat kodeksiga nafaqat "kompyuter texnikasi vositalari", balki "raqamli aktivlar, virtual valyutalar va sun'iy intellekt texnologiyalaridan foydalangan holda" degan og‘irlashtiruvchi normalarni kiritish lozim.

Kvalifikatsiya mezonlarini aniqlashtirish: Tizimga ruxsatsiz kirib pul yechib olish holatlarini faqatgina firgarlik (168-modda) emas, balki axborot tizimlariga noqonuniy kirish (278-1-modda) va o‘g‘rilik (169-modda) moddalari bilan to‘g‘ri kombinatsiyalash mexanizmini O‘zbekiston Respublikasi Oliy sudi Plenumi qarorida aks ettirish zarur.

Xalqaro hamkorlik: Kiberfirgarlikning transchegaraviy tabiatini inobatga olib, elektron dalillarni tezkor almashish bo‘yicha xalqaro konvensiyalarga integratsiyalashuvni kuchaytirish lozim.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasining Jinoyat kodeksi. – Toshkent: Adolat, 2025.
2. Rustambayev M.X. O‘zbekiston Respublikasi Jinoyat huquqi kursi. III jild: Mulkka qarshi jinoyatlar. – Toshkent: Ilm-ziyo, 2018.
3. Yakubova S.S. Kiberjinoyatchilikning jinoiy-huquqiy va kriminologik jihatlari. Huquq va burch jurnali. – 2022. – №4. – B. 22-27.
4. Karimov A.A. Kompyuter texnikasi vositalaridan foydalanib sodir etiladigan firgarlikni kvalifikatsiya qilish muammolari. // O‘zbekiston qonunchiligi tahlili. – 2023. – №2. – B. 45-51.
5. Council of Europe. Convention on Cybercrime (Budapest Convention). – Budapest, 23.XI.2001.
6. Brenner, S. W. Cybercrime: Criminal Threats to the Information Age. – Greenwood Publishing Group, 2010.
7. Grabosky, P. Cybercrime (Key广 Concepts in Criminology). – Oxford University Press, 2016.
8. Smith, R. G., Grabosky, P., & Urbas, G. Cyberlines: Crime in the Digital Age. – Palgrave Macmillan, 2021.
9. Ivanov N.G. Kibermoshennichestvo kak ugroza ekonomicheskoy bezopasnosti. Ugolovnoye pravo (Rossiya). – 2021. – №5. – S. 12-19.
10. O‘zbekiston Respublikasi Oliy sudi Plenumi Qarori "Sudlar tomonidan firgarlik jinoyatlariga oid qonunchilikni qo‘llash amaliyoti to‘g‘risida" (Yangi tahriri loyihalari va sharhlari, 2024).