# LEGAL ANALYSIS OF CYBER FRAUD: UZBEKISTAN AND FOREIGN EXPERIENCE

**Hamidova Sohiba Sohib qizi**

Master's Student, Cyber Law Program Tashkent State University of Law

E-mail: sohibahamidova48@gmail.com

**Annotation**

This article provides a comparative legal analysis of the legal nature and the elements of the corpus delicti of cyber fraud, based on the criminal legislation of the Republic of Uzbekistan and that of foreign countries (the Russian Federation, the Federal Republic of Germany, and the Republic of Korea). The study reveals the concept of cyber fraud and its most widespread types (phishing, social engineering), and examines in detail the object, objective side, subject, and subjective side of the crime. The qualification of cyber fraud under Article 168 of the current Criminal Code is analysed, and it is substantiated that in foreign countries this act is regulated as an independent corpus delicti. As a result, conclusions are formulated on improving the criminal legislation of Uzbekistan.

**Keywords**

cyber fraud, corpus delicti, object, objective side, subject, subjective side, phishing, social engineering.

## KIBERFIRIBGARLIK JINOYATINING YURIDIK TAHLILI: O‘ZBEKISTON VA XORIJIY TAJRIBA

*Hamidova Sohiba Sohib qizi*

*Toshkent davlat yuridik universiteti Kiber huquqi mutaxassisligi magistranti*

**Annotatsiya.** Mazkur maqolada kiberfiribgarlik jinoyatining yuridik tabiati, uning jinoyat tarkibi belgilari O‘zbekiston Respublikasi jinoiy qonunchiligi hamda xorijiy davlatlar (Rossiya Federatsiyasi, Germaniya Federativ Respublikasi, Janubiy Koreya

Respublikasi) qonunchiligi misolida qiyosiy-huquqiy jihatdan tahlil qilingan. Tadqiqotda kiberfiribgarlik tushunchasi, uning eng keng tarqalgan turlari (fishing, ijtimoiy muhandislik) ochib berilgan, jinoyatning obyekti, obyektiv tomoni, subyekti va subyektiv tomoni batafsil tadqiq etilgan. Amaldagi Jinoyat kodeksining 168-moddasi bo‘yicha kiberfiribgarlik kvalifikatsiyasi tahlil qilinib, xorijiy davlatlarda mazkur qilmish mustaqil jinoyat tarkibi sifatida tartibga solinganligi asoslangan. Tadqiqot natijasida O‘zbekiston jinoiy qonunchiligini takomillashtirish bo‘yicha xulosalar shakllantirilgan.

**Kalit so‘zlar:** kiberfiribgarlik, jinoyat tarkibi, obyekt, obyektiv tomon, subyekt, subyektiv tomon, fishing, ijtimoiy muhandislik.

**Аннотация.** В данной статье осуществлен сравнительно-правовой анализ юридической природы кибермошенничества и признаков его состава на примере уголовного законодательства Республики Узбекистан и зарубежных стран (Российской Федерации, Федеративной Республики Германия, Республики Корея). В исследовании раскрывается понятие кибермошенничества, его наиболее распространенные виды (фишинг, социальная инженерия), а также детально исследуются объект, объективная сторона, субъект и субъективная сторона данного преступления. Проанализирована квалификация кибермошенничества по статье 168 действующего Уголовного кодекса и обосновано, что в зарубежных странах данное деяние регламентировано в качестве самостоятельного состава преступления. По результатам исследования сформулированы выводы по совершенствованию уголовного законодательства Узбекистана.

**Ключевые слова:** кибермошенничество, состав преступления, объект, объективная сторона, субъект, субъективная сторона, фишинг, социальная инженерия.

**Kirish.** Axborot-kommunikatsiya texnologiyalarining hayotning barcha jabhalariga jadal kirib borishi va masofaviy bank xizmatlarining ommalashuvi natijasida an'anaviy firibgarlik o'zining sodir etilish usuli va vositasi jihatidan tubdan o'zgardi hamda kiberfiribgarlik qilmishlarining ko'payishiga zamin yaratdi. O'zbekiston Respublikasi Ichki ishlar vazirligi Kiberxavfsizlik markazining ma'lumotlariga ko'ra, 2024-yilda axborot texnologiyalaridan foydalanib 58 800 ta qilmish qayd etilgan bo'lib, bu ko'rsatkich besh yil ichida 68 barobarga oshgan. O'zbekiston fuqarolari so'nggi besh yilda kiberfiribgarliklar oqibatida shaxsiy hisoblaridan umumiy hisobda 159 million AQSh dollariga teng mablag'ni yo'qotgan[1]. Ushbu raqam mamlakatda raqamli moliyaviy xavfsizlikka bo'lgan tahdidning jiddiy darajada o'sib borayotganidan dalolat beradi. Global miqyosda kiberfiribgarlikning fishing turi 2025-yilda ham eng keng tarqalgan turi bo'lib, u barcha kiberhujumlarning 39 foizini tashkil etgan. Yoki ijtimoiy muhandislik usullari orqali (jumladan, mijozlarni qo'llab-quvvatlash xizmatining soxta xodimlari va kompaniya vakillari) hajmi 2025-yilda butun dunyo bo'ylab 92 foizga oshdi[2]. Mazkur raqamlar kiberfiribgarlikka qarshi samarali jinoiy-huquqiy kurash choralarini ishlab chiqish dolzarb ilmiy-amaliy vazifa ekanligidan dalolat beradi. Shu munosabat bilan mazkur maqolaning maqsadi - kiberfiribgarlikning jinoyat tarkibi belgilarini O'zbekiston va xorijiy davlatlar qonunchiligi misolida qiyosiy-huquqiy jihatdan tahlil qilish hamda milliy qonunchilikni takomillashtirish bo'yicha xulosalar shakllantirishdan iborat.

**Tadqiqot metodologiyasi:**Tadqiqotda normativ-huquqiy tahlil, doktrinal tahlil, qiyosiy-huquqiy va tizimli-strukturaviy usullardan foydalanildi. Normativ-huquqiy tahlil yordamida O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasi va Oliy sud Plenumining firibgarlikka oid qarori o'rganildi. Qiyosiy-huquqiy usul Rossiya Federatsiyasi, Germaniya Federativ Respublikasi va Janubiy Koreya Respublikasi jinoiy qonunchiligidagi kiberfiribgarlikka oid normalarni milliy qonunchilik bilan qiyoslashda

qo‘llanildi. Tadqiqotning empirik bazasini huquqni muhofaza qiluvchi organlarning statistik ma’lumotlari, doktrinal manbalar va xorijiy davlatlarning jinoyat kodekslari tashkil etadi.

**Adabiyotlar tahlili:** Kiberfiribgarlik jinoyati uchun javobgarlik belgilash mavzusi ko‘pincha ilmiy adabiyotlarda kiberjinoyatchilik, an’anaviy firibgarlik doirasida o‘rganilib tahlil qilingan mavzu hisoblanadi. Mazkur sohaning fundamental muammolari va rivojlanish dinamikasini tushunish uchun xalqaro va milliy doktrinal manbalarning yondashuvlarini tahlil qilish lozim. Kiberfiribgarlik muammosining xalqaro doktrinal jihatlarini tahlil qilishda zamonaviy kriminologiyaning yetakchi namoyandalaridan biri, Kardiff universiteti professori Maykl Levining (Michael Levi) tadqiqotlari alohida ahamiyat kasb etadi. Uning hammualliflikda chop etilgan “Kiberfiribgarlik va samarali xavfga asoslangan javob choralari uchun uning oqibatlari: Buyuk Britaniya tadqiqotidan kelib chiqqan masalalar” nomli maqolasi mazkur yo‘nalishdagi eng nufuzli empirik tadqiqotlardan biri hisoblanadi. Tadqiqotda mualliflar “kiberfiribgarlik” (cyberfraud) tushunchasini *kiber o‘lchovga ega firibgarlik* sifatida ta’riflaydilar. Levi kiberfiribgarlikning eng muhim o'ziga xos xususiyati sifatida jinoyatchining joylashgan o‘rni hech qanday tabiiy hududiy chegaraga ega emasligini ko‘rsatadilar. Shu bilan birga, mualliflar kiberfiribgarlikning barchasi ham transmilliy xarakterga ega emas, chunki ayrim hollarda jinoyat sikllarining muayyan bosqichida bevosita yuzma-yuz muloqot saqlanib qoladi, onlayn auksion savdosidagi firibgarliklarda esa jinoyatchi va jabrlanuvchi ko‘pincha bir mamlakatda istiqomat qilishini ta’kidlaydilar. Milliy olimlardan **H.R. Ochilov** o‘zgalar mulkini kompyuter vositalari orqali talon-toroj qilishga qarshi kurash bilan bog‘liq munosabatlar tizimini tadqiqot obyekti sifatida belgilaydi o‘rganib, muallif axborot texnologiyalari yordamida sodir etiladigan jinoyatlarning mexanizmi va usullarini tasniflab, kompyuter firibgarligi deganda moliya, bank muassasalari va fondlardagi mulkni aldov yo'li bilan kompyuter

texnikasi vositalari yordamida manipulyatsiya qilish orqali amalga oshiriladigan talon-torojni tushunish lozimligini asoslaydi; bunday firibgarlik kompyuter tizimida ishlov beriladigan, axborot tashuvchilarda saqlanadigan yoki uzatish tarmoqlari bo'yicha beriladigan axborotni o'zgartirish, shuningdek, tizimga yolg‘on axborot kiritish yo‘li bilan ham sodir etilishi mumkinligini ko‘rsatadi. Tadqiqotning eng muhim amaliy natijasi sifatida muallif o‘zgalar mulkini kompyuter vositalaridan foydalanib talon-toroj qilganlik uchun Jinoyat kodeksida **alohida moddada javobgarlik belgilash** hamda Oliy sud Plenumining tegishli qarorini ishlab chiqishga doir takliflarni ilgari suradi. Shu o‘rinda ta’kidlash joizki, Ochilovning yondashuvi mulkiy jinoyatlarning keng doirasini “kompyuter vositasidan foydalanib talon-toroj qilish” yagona kategoriyasi ostida – ya’ni *kompyuter vosita (qurol) sifatida foydalaniladigan* (cyber-enabled) jinoyatlar konsepsiyasi asosida birlashtirishga tayanadi. **S.G‘. Isomiddinov** firibgarlik qurbonlarining xulq-atvori, individual viktimologik omillari hamda ularning jinoyat mexanizmidagi rolini tadqiq etadi. Muallif viktimologik profilaktika amaldagi qonunchilik doirasidagi chora-tadbirlar bilan cheklanmasligi, balki jinoyatchilikning zamonaviy tendensiyalaridan kelib chiqib ta'sir usullarini qamrab olishi zarurligini asoslaydi. Shu bilan birga, Isomiddinov ishi jinoyatning oldini olish va profilaktika choralarini chuqur yoritsa-da, kiberfiribgarlikni kvalifikatsiya qilishning moddiy-huquqiy asoslari uning tadqiqot doirasidan tashqarida qoladi.

**Tahlil va natijalar:** Bugungi kunda G‘arbiy davlatlar, AQSh, Yevropa va Rossiyada kompyuter yordamida sodir etilayotgan firibgarlik jinoyatlari “kompyuter firibgarligi”, “Internet firibgarligi”, “kompyuter axboroti sohasidagi firibgarlik” va “kiberfiribgarlik” degan nomlar bilan atalmoqda. Olimlarning fikricha, bu tushunchalar mazmunan bir xil ma’noga ega. Kiberfiribgarlik kompyuter, Internet yoki boshqa elektron resurs, vositadan foydalangan holda o‘zgalar mulkini aldash yoki ishonchini suiiste’mol qilish yo‘li bilan jabrlanuvchiga moddiy zarar yetkazishdir. Xorijiy

doktrinada M.Button va C.Cross kiberfiribgarlikni inson omilini aldashga asoslangan “kiber-imkoniyatli” (cyber-enabled) kiberjinoyat turiga kiritadilar(. Kiberfiribgarlikning mohiyati shundaki, an’anaviy firibgarlikdagi kabi mol-mulk jabrlanuvchi tomonidan, aldov ta’sirida xato tasavvur hosil qilish tufali ixtiyoriy tarzda jinoyatchiga o‘tkazib beriladi. Aynan shu “ixtiyoriy o‘tkazish” mezoni kiberfiribgarlikni kiber-o‘g‘rilik va boshqa axborotlashtirish sohasidagi qilmishlaridan ajratib turadi.

Hozirgi kunda kiberfiribgarlikning eng keng tarqalgan turlari fishing va ijtimoiy muhandislik (social engineering) usullaridir. *Fishing* - jabrlanuvchini bank, davlat xizmati yoki tashkilot nomidan yuborilgan soxta xat, xabar yoki saytga jalb qilib, undan bank kartasi rekvizitlari, kodlari kabi maxfiy ma’lumotlarini qo‘lga kiritish usulidir. Ya’ni bunda jinoyatchilar jabrlanuvchini shubhali havolalar orqali mobil telefoniga ulanib, undan shaxsga doir ma’lumotlar, bank karta rekvizitlarini qo‘lga kiritib, so‘ng ular yordamida jabrlanuvchining nomiga bankdan kredit rasmiylashtirishi, yoki bank hisobvarag‘idan pullarini o‘zlashtiradi. Shuningdek, yana bir eng ommabop usullaridan biri ijtimoiy muhandislik bo‘lib, bunda jinoyatchi texnik vositalarni buzishdan ko‘ra, inson psixologiyasiga ta’sir o‘tkazib, jabrlanuvchini o‘zi xohlagan harakatni (pul o‘tkazish, ma’lumot berish) bajarishga undash usulidir. Bunga huquqni muhofaza qiluvchi organ, bank yoki ish beruvchi xodimi nomidan qo‘ng‘iroq qilib psixologik bosim o‘tkazish, tanish-bilish nomidan shoshilinch pul so‘rash, meros yoki lotereya yutuqlari bilan aldash kabi sxemalar kiradi. So‘nggi yillarda firibgarlar sun’iy intellekt yordamida akkaunt egasi nomidan soxta audio- va videoxabarlar yaratish, soxta onlayn-do‘konlar tashkil etish hamda kriptovalyuta investitsiyasi niqobidagi sxemalardan ham keng foydalanmoqda[4; 36 b].

Bugungi kunda amaldagi qonunchilikka ko‘ra kiberfiribgarlik qilmishi O‘zbekiston Respublikasi Jinoyat kodeksining 168-modda uchinchi qismining “g” bandi bo‘yicha kvalifikatsiya qilinadi, bunda axborot tizimi, axborot texnologiyalaridan

foydalanib sodir etilgan firibgarlik an’anaviy firibgarlik uchun og‘irlashtiruvchi holati sifatida baholanadi[5]. 168-moddaga muvofiq, firibgarlik - aldash yoki ishonchni suiiste’mol qilish yo‘li bilan o‘zganing mol-mulkini yoki mol-mulkka bo‘lgan huquqini egallashdir. O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-son qarorida quyidagicha tushuntirish beriladi: “*axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib firibgarlik sodir etish (JK 168-moddasi uchinchi qismi “g” bandi) deganda, moliya, bank muassasalari, fondlar va sh.k. larda bo‘lgan mulkni aldov yo‘li bilan kompyuter texnikasi vositalari, aloqa vositasi, planshet yoki boshqa shu kabi texnik qurilmalar yordamida manipulatsiya qilish orqali amalga oshiriladigan talon-toroj tushuniladi. Bunday firibgarlik kompyuter tizimida ishlov beriladigan, tegishli axborot tashuvchilarda saqlanadigan yoki ma’lumotlarni uzatish tarmoqlari bo‘yicha beriladigan axborotni o‘zgartirish yo‘li bilan ham, kompyuter tizimiga yolg‘on axborot kiritish yo‘li bilan ham sodir etilishi mumkin*”[6]. Kiberfiribgarlik jinoyati an’anaviy firibgarlikdan farqli ravishda bir necha o‘ziga xos xususiyatlarga ega, xususan, uning axborot texnologiyalaridan foydalanib sodir etilishi natijasida jinoyatchilarning anonimligi yuqori bo‘lishi, jinoyat kibermuhitda sodir bo‘lishi va bu jinoyatchidan ham, huquqni muhofaza qiluvchi organ vakillaridan ham maxsus bilimlarga ega bo‘lishni talab qilishi, jinoyatchi bir vaqtning o‘zida yuz, minglagan shaxslarga mulkiy zarar yetkaza oladi. Kiberfiribgarlik jinoyatini jinoiy tarkibini tahlil qiladigan bo‘lsak, kiberfiribgarlikning obyekti xususida olimlar turli fikrlarni bildirishgan bo‘lib, masalan, O.M. Safonov jinoyatni ikki obyektli deb belgilaydi: mulk va kompyuter tizimlari xavfsizligi[7]. T.M. Lopatina asosiy obyektni mulk, fakultativ obyektni esa kompyuter ma’lumotlari sohasidagi munosabatlar deb biladi[8]. V.T.Tomina, V.V.Sverchkova, A.V.Brilliantov, G.D.Doljenkova, E.N.Jevlakov, milliy olimlardan M.Rustambayev, D.Saidov va boshqalar o‘zlarining

sharhlari hamda kitoblarida kompyuter firibgarligining jinoyat obyekti sifatida o‘zgalar mol-mulkini belgilashadi [9;10,11].Darhaqiqat, kiberfiribgarlik bir vaqtning o‘zida bir nechta ijtimoiy munosabatlarga tajovuz qiladi. Uning tabiatidan kelib chiqib bevosita asosiy obyektini mulkiy munosabatlar shaxs yoki tashkilotning mol-mulkka bo‘lgan egalik, foydalanish va tasarruf etish huquqi tashkil etadi. Fakultativ qo‘shimcha obyektini esa axborot xavfsizligi sohasidagi munosabatlar axborot tizimlari, elektron ma’lumotlar va raqamli infratuzilmaning butunligi va ishonchliligi tashkil etadi. Kiberfiribgarlikning obyektiv tomoni an’anaviy firibgarlikning obyektiv tomoni mohiyati bilan ayni bo‘lib, uning raqamli texnologiyalardan foydalanib kibermuhitda sodir bo‘lishi bilan farq qiladi. Ya’ni axborot texnologiyalari vositasida amalga oshiriladigan aldash yoki ishonchni suiiste’mol qilish harakatida, uning natijasida jabrlanuvchining mol-mulki yoki mol-mulkka bo‘lgan huquqining jinoyatchiga o‘tishida hamda shu harakat bilan oqibat o‘rtasidagi sababiy bog‘lanishda namoyon bo‘ladi. Jinoyat Kodeksimizga ko‘ra kiberfiribgarlikning subyekti qilmish sodir etilgan paytda o‘n olti yoshga to‘lgan, aqli raso jismoniy shaxsdir[12]. Subyektning o‘ziga xosligi shundaki, kiberfiribgarlik ko‘pincha texnik bilim va ko‘nikmaga ega shaxslar, shuningdek uyushgan guruh yoki transmilliy jinoiy tarmoqlar tomonidan, rollar taqsimoti asosida (biri texnik ta’minot, ikkinchisi jabrlanuvchi bilan muloqot, uchinchisi pul mablag‘ini legalizatsiya qilish bilan shug‘ullanadi) sodir etiladi. Bu hol javobgarlikni og‘irlashtiruvchi belgi sifatida e’tirof etilishi lozim. Kiberfiribgarlik faqat to‘g‘ri qasd bilan sodir etiladi, ya’ni jinoyatchi o‘z qilmishining ijtimoiy xavfli ekanligini anglaydi, jabrlanuvchiga mulkiy zarar yetkazishni va shu yo‘l bilan o‘ziga yoki uchinchi shaxsga noqonuniy mulkiy naf keltirishni xohlaydi. Chunki sun’iy intellekt orqali ma’lum bir odamlarni shaxsini, ovozi yoki ko‘rinishini o‘xshatish orqali odamlardan mulkiy manfaat ko‘zlash yoki telefon orqali o‘zini bank yoki davlat organi xodimi sifatida tanishtirib inson psixologiyasi – ishonchi, qo‘rquvi, tez boyish istagi –

kabi omillarni ishga solishi faqatgina ongli amalga oshirilishi mumkin. Mazkur belgilar kiberfiribgarlikni ehtiyotsizlik orqali sodir etiladigan qilmishlardan va yondosh axborotlashtirish sohasidagi huquqbuzarliklaridan ajratib turadi.

Ayrim rivojlangan davlatlar qonunchiligida kiberfiribgarlik (kompyuter firibgarligi) an'anaviy firibgarlikdan ajratilib, alohida mustaqil modda bilan tartibga solinadi. Xususan, huquqiy tizimi bizniki bilan o'xshash bo'lgan Rossiya Federatsiyasi Jinoyat kodeksida firibgarlikning maxsus turlari alohida moddalarga ajratilgan. $159^3$-modda elektron to'lov vositalaridan foydalangan holda firibgarlik uchun, $159^6$-modda esa kompyuter axboroti sohasidagi firibgarlik, ya'ni kompyuter axborotini kiritish, o'chirish, bloklash, o'zgartirish yoki axborot tizimlari ishiga boshqacha tarzda aralashish yo'li bilan o'zganing mol-mulkini egallash yoki mol-mulkka bo'lgan huquqni qo'lga kiritish uchun javobgarlikni belgilaydi[13]. Rossiya doktrinasida (S.V.Sheveleva, A.V.Yujin, M.A.Yefremova) ushbu maxsus normalarning kvalifikatsiyadagi ahamiyati keng tahlil qilingan. Shuningdek, Germaniya Jinoyat kodeksi (StGB) kompyuter firibgarligini (Computerbetrug) 263a-paragrafda alohida tartibga soladi. Ushbu norma an'anaviy firibgarlikdan shu bilan farq qiladiki, unda aldash insonga emas, balki ma'lumotlarni qayta ishlash jarayoniga (avtomatlashtirilgan tizimga) noto'g'ri yoki to'liq bo'lmagan ma'lumot kiritish, ruxsatsiz ma'lumotlardan foydalanish yo'li bilan ta'sir ko'rsatiladi. 263a-paragrafga muvofiq, kompyuter firibgarligi jarima yoki besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi, alohida og'ir holatlarda (uyushgan guruh tomonidan, kasb-hunar sifatida yoki katta miqdorda zarar yetkazib sodir etilganda) jazo olti oydan o'n yilgacha ozodlikdan mahrum qilishni tashkil etadi [14]. Muhimi, Germaniya qonunchiligida kompyuter firibgarligini sodir etish uchun mo'ljallangan dasturlarni tayyorlash yoki tarqatish kabi tayyorgarlik harakatlari ham (263a-paragraf 3-qismi) jinoiy javobgarlikka tortiladi. Kiberfiribgarlikni mustaqil norma sifatida belgilagan davlatlardan yana biri Janubiy

Koreya bo‘lib, Jinoyat Kodeksning 347-modda (Firibgarlik) umumiy firibgarlik uchun, 347-2-modda (Kompyuter va shu kabilardan foydalangan holda firibgarlik) esa maxsus kiberfiribgarlik uchun javobgarlikni belgilaydi. 347-2-moddaga muvofiq, kompyuter va shunga o‘xshash ma’lumot qayta ishlash qurilmasiga yolg‘on ma’lumot yoki noto‘g‘ri buyruq kiritish, yoxud ruxsatsiz ma’lumot kiritish yoki o‘zgartirish orqali mulkiy naf olish yoki uchinchi shaxsga mulkiy naf keltirish o‘n yilgacha ozodlikdan mahrum qilish yoki yigirma million von miqdorigacha jarima bilan jazolanadi [15]. Bu norma ham Germaniya modelidagi kabi, aldovning inson emas, balki avtomatlashtirilgan tizimga qaratilganligini hisobga oladi.

Qiyosiy tahlil shuni ko‘rsatadiki, uchala davlatda ham kiberfiribgarlik (kompyuter firibgarligi) an’anaviy firibgarlikdan ajratilib, mustaqil jinoyat tarkibi sifatida tartibga solinadi va unga mutanosib jazo belgilanadi. Bundan tashqari, 2024-yil 24-dekabrda BMT Bosh Assambleyasi tomonidan qabul qilingan “Kiberjinoyatchilikka qarshi konvensiyasi”ning 13-moddasi ham aynan axborot tizimlari bilan bog‘liq firibgarlikni mustaqil jinoyat sifatida belgilashni nazarda tutadi [16]. Bu kiberfiribgarlikni mustaqil tarkib sifatida ajratish global huquqiy tendensiya ekanligini tasdiqlaydi. O‘zbekiston Respublikasida esa mazkur qilmish hanuzgacha og‘irlashtiruvchi holat darajasida tartibga solinmoqda, bu esa huquqni qo‘llash amaliyotida vujudga kelayotgan ba’zi tushunmovhciliklarni bartaraf etish hamda shaxsga nisbatan qo‘llanilayotgan sanksiya adolatli bo‘lishi uchun kiberfiribgarlik jinoyati qonunchilikda yetarlicha to‘liq kiritilish kerak.

**Xulosa va takliflar.** Olib borilgan qiyosiy-huquqiy tahlil quyidagi xulosalarga olib keldi. Birinchidan, kiberfiribgarlik o‘ziga xos tabiatga, masofaviy va transchegaraviy obyektiv tomonga hamda ko‘pincha uyushgan-transmilliy subyektga ega bo‘lib, u an’anaviy firibgarlikdan sifat jihatidan farq qiladigan mustaqil ijtimoiy-huquqiy hodisadir. Ikkinchidan, uning eng keng tarqalgan turlari (fishing, ijtimoiy muhandislik)

asosida inson omilini aldash yotadi. Uchinchidan, Rossiya Federatsiyasi (159³, 159⁶-moddalar), Germaniya Federativ Respublikasi (263a-paragraf) va Janubiy Koreya Respublikasi (347-2-modda) tajribasi kiberfiribgarlikni mustaqil jinoyat tarkibi sifatida tartibga solish samarali huquqiy yechim ekanligini ko‘rsatadi. Mazkur xorijiy tajriba hamda BMT Kiberjinoyatchilik konvensiyasining 13-moddasidagi xalqaro standart asosida O‘zbekiston Respublikasi Jinoyat kodeksiga kiberfiribgarlik uchun javobgarlikni nazarda tutuvchi mustaqil modda kiritish maqsadga muvofiqdir. Bunday norma qilmishning obyektiv va subyektiv belgilarini aniq belgilashi, og‘irlashtiruvchi holatlar (uyushgan guruh, transchegaraviy sodir etish, maxsus texnik vositalar va soxta shaxsiy ma’lumotlardan foydalanish) hamda mutanosib jazo choralarini o‘z ichiga olishi lozim. To‘rtinchidan, kiberfiribgarlik jinoyatni tahlil qilib borilishi, ya’ni firibgarlar tomonidan qaysi shakldagi sxemalardan foydalangan holda firibgarlik jinoyatini sodir etilayotganligini aniqlash, va u haqida vaqtida butun aholini ogohlantirib turish maqsadida Kiberxavfsizlik markazi DUK platformasida alohida kiberfiribgarlik qurbonlari murojaat qilishi mumkin bo‘lgan onlayn shikoyatlar darchasini ajratish maqsadga muvofiq.

## FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Zamin.uz internet nashrining maqolasi // https://zamin.uz/uz/ozbekiston/166748/html.

2. “SQmagazine” internet nashrining 2026-yildagi kiberjinoyatlar statistikasi // https://sqmagazine.co.uk/cybercrime-statistics/#Global-Cybercrime-Incidence-Rates.

3. McGuire M., Dowling S.(2013). Cyber crime: A review of the evidence // Home Office Research Report 75. - London, p 42.

4. Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge, p 236.

5. O‘zbekiston Respublikasining Jinoyat kodeksi // lex.uz - O‘zbekiston Respublikasi Qonunchilik ma’lumotlari milliy bazasi

6. O‘zbekiston Respublikasi Oliy Sudi Plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-son Qarori // O‘zbekiston Respublikasi qonunchilik hujjatlari ma’lumotlari milliy bazasi.

7. Сафонов О.М.(2015). Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и право применительной практики, перспективы совершенствования : дис. канд. юрид. наук : 12.00.08 / О.М. Сафонов. – Москва, - С. 115-116.

8. Лопатина Т.М. (2013). Проблемы уголовно-правовой защиты сферы компьютер ной информации: современный взгляд на мошенничество. Право и безопасность.- № 3-4 (45). - С. 93.

9. В.Т.Томина, В.В.Сверчкова (2019). Комментарий к Уголовному кодексу Российкой Федерации. В 3 т. Т. 2. Особенная часть. Разделы VII-VIII / под ред. -

10-е изд., перераб. и доп. - М.: Издательство Юрайт, - С. 159. -Серия: Профессиональные комментарии.

10. Г.Д.Долженкова, Э.Н.Жевлаков (и др.) (2017) Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2т. /

11. А.В.Бриллиантов, под ред. А.В.Бриллиантова. - 2-е изд. - Москва: Проспект, С. 599-606.

12. Rustambayev M.X. (2018) O‘zbekiston Respublikasi jinoyat huquqi kursi. Tom 1. Jinoyat haqida ta’limot. Darslik. 2-nashr, to‘ldirilgan va qayta ishlangan - T.: O‘zbekiston Respublikasi Milliy gvardiyasi Harbiy-texnik instituti, 170b.

13. Rossiya Federatsiyasi Jinoyat Kodeksi // https://ivo.garant.ru/#/document/10108000/paragraph/ 42618272:0

14. Germaniya Jinoyat kodeksi // https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

15. Janubiy Koreya Jinoyat kodeksi // https://www.law.go.kr/LSW/eng/engLsInfoR.do?lsiSeq=253323.

16. United Nations Office on Drugs and Crime(UNODC). (2024). *United Nations Convention Against Cybercrime*. https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html