RAQAMLI MAKONDA KIBERFIRIBGARLIK JINOYATLARINI KVALIFIKATSIYA QILISH MUAMMOLARI

Anorboyev Murodjon Raxmanqul o`g`li
Tashkent International University
“Huquqiy fanlar kafedrasi”
dotsenti vazifasini bajaruvchisi yu.f.f.d., (PhD)
E-mail: m0116anomura@mail.ru

Ziyovuddinova Madina Kamoliddin qizi
Tashkent International University
Yurisprudensiya yo’nalishi 2-bosqich talabasi
E-mail:Ziyovutdinovamadina1808@gmail.com
Tel:+998949069025
https://doi.org/10.5281/zenodo.20363616

ANOTATSIYA

Mazkur ilmiy maqolada raqamli muhitda sodir etilayotgan kiberfiribgarlik jinoyatlarining huquqiy tabiati, ularni kvalifikatsiya qilishdagi dolzarb muammolar hamda jinoyat huquqi normalari asosida javobgarlik masalalari kompleks tarzda tahlil qilinadi. Tadqiqot davomida kiberfiribgarlik tushunchasining mazmuni, uning an’anaviy firibgarlikdan farqli jihatlari, jinoyat tarkibining obyektiv va subyektiv belgilari yoritiladi. Shuningdek, O‘zbekiston Respublikasi Jinoyat kodeksining tegishli moddalarini qo‘llash amaliyotida yuzaga kelayotgan muammolar, xususan, jinoyatni to‘g‘ri kvalifikatsiya qilish, zarar yetkazish usullari, axborot texnologiyalaridan foydalanish orqali sodir etilgan firibgarliklarni huquqiy baholashdagi ziddiyatlar ko‘rib chiqiladi.

Maqolada sud amaliyoti va plenum qarorlari asosida huquqni qo‘llashdagi mavjud kamchiliklar tahlil qilinib, ularni bartaraf etish bo‘yicha ilmiy asoslangan taklif va tavsiyalar ilgari suriladi. Bundan tashqari, kiberjinoyatchilikka qarshi kurashishda zamonaviy yondashuvlar, xalqaro tajriba va milliy qonunchilikni takomillashtirish zarurati asoslab beriladi. Tadqiqot natijalari raqamli iqtisodiyot sharoitida jinoyat huquqini rivojlantirish va amaliyotini takomillashtirishga xizmat qiladi.

KALIT SO‘ZLAR: kiberfiribgarlik, raqamli muhit, jinoyat huquqi, kvalifikatsiya muammolari, javobgarlik, jinoyat tarkibi, axborot texnologiyalari, firibgarlik usullari, sud amaliyoti, plenum qarorlari, huquqiy normalar, kiberjinoyatchilik, elektron to‘lovlar, zarar yetkazish, huquqni qo‘llash amaliyoti.

КИБЕРМОШЕННИЧЕСТВО В ЦИФРОВОЙ СРЕДЕ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ВОПРОСЫ ОТВЕТСТВЕННОСТИ

АННОТАЦИЯ

В данной научной статье комплексно анализируются правовая природа преступлений кибермошенничества, совершаемых в цифровой среде, актуальные проблемы их квалификации, а также вопросы уголовной ответственности на основе норм уголовного права. В ходе исследования раскрывается содержание понятия кибермошенничества, его отличительные особенности по сравнению с традиционным мошенничеством, а также объективные и субъективные признаки состава преступления. Кроме того, рассматриваются проблемы, возникающие в правоприменительной практике при применении соответствующих норм Уголовного

кодекса Республики Узбекистан, в частности вопросы правильной квалификации преступлений, способов причинения ущерба, а также правовой оценки мошенничества, совершённого с использованием информационных технологий.

В статье на основе анализа судебной практики и постановлений Пленума рассматриваются существующие недостатки правоприменения и выдвигаются научно обоснованные предложения и рекомендации по их устранению. Также обосновывается необходимость современных подходов в противодействии киберпреступности, изучения международного опыта и совершенствования национального законодательства. Результаты исследования направлены на развитие уголовного права и совершенствование его практического применения в условиях цифровой экономики.

КЛЮЧЕВЫЕ СЛОВА:кибермошенничество, цифровая среда, уголовное право, проблемы квалификации, ответственность, состав преступления, информационные технологии, способы мошенничества, судебная практика, постановления Пленума, правовые нормы, киберпреступность, электронные платежи, причинение ущерба, правоприменительная практика.

CYBER FRAUD IN THE DIGITAL ENVIRONMENT: CURRENT ISSUES OF QUALIFICATION AND CRIMINAL LIABILITY

ABSTRACT

This scientific article provides a comprehensive analysis of the legal nature of cyber fraud crimes committed in the digital environment, the current challenges in their qualification, and issues of criminal liability based on the norms of criminal law. The study examines the content of the concept of cyber fraud, its distinctive features compared to traditional fraud, as well as the objective and subjective elements of the corpus delicti. Furthermore, it addresses the problems arising in law enforcement practice in the application of the relevant provisions of the Criminal Code of the Republic of Uzbekistan, in particular issues related to the correct legal qualification of offenses, methods of causing damage, and the legal assessment of fraud committed through the use of information technologies.

The article, based on the analysis of judicial practice and Plenum resolutions, identifies existing shortcomings in law enforcement and proposes scientifically grounded recommendations and suggestions for their elimination. It also substantiates the necessity of modern approaches in combating cybercrime, the study of international experience, and the improvement of national legislation. The findings of the research are aimed at the development of criminal law and the enhancement of its practical application in the context of the digital economy.

KEYWORDS:cyber fraud, digital environment, criminal law, qualification issues, liability, corpus delicti, information technologies, methods of fraud, judicial practice, Plenum resolutions, legal norms, cybercrime, electronic payments, damage causation, law enforcement practice.

KIRISH

Raqamli iqtisodiyotning jadal rivojlanishi, internet va mobil texnologiyalarning keng ommalashuvi jamiyat hayotining barcha sohalariga chuqur kirib bordi. Shu bilan birga, axborot-kommunikatsiya texnologiyalaridan noqonuniy foydalanish orqali sodir etilayotgan jinoyatlar, xususan, kiberfiribgarlik holatlarining keskin ortishi kuzatilmoqda. Bugungi kunda firibgarlikning an’anaviy shakllari bilan bir qatorda, elektron to‘lov tizimlari, ijtimoiy tarmoqlar, onlayn savdo platformalari va bank xizmatlari orqali amalga oshiriladigan yangi

usullari paydo bo‘lmoqda. Bu esa jinoyat huquqi nazariyasi va amaliyotida mazkur turdagi jinoyatlarni to‘g‘ri kvalifikatsiya qilish, ularning huquqiy chegaralarini aniqlash hamda samarali javobgarlik choralarini qo‘llash masalalarini dolzarb etib qo‘ymoqda. O‘zbekiston Respublikasida kiberfiribgarlikka qarshi kurashish Jinoyat kodeksining bir qator moddalarida, xususan, 168-modda (firibgarlik), 169-modda (o‘g‘rilik), 278⁶-modda (axborot texnologiyalaridan foydalanib sodir etiladigan jinoyatlar) kabi normalar orqali tartibga solinadi[1]. Biroq amaliyotda mazkur moddalarning qo‘llanishi bir qator muammolarni keltirib chiqarmoqda. Jumladan, jinoyatni sodir etish usuli (onlayn yoki an’anaviy), jinoyat predmeti (pul mablag‘lari, elektron aktivlar), shuningdek, jinoyat sodir etishda foydalanilgan vositalarning o‘ziga xosligi kvalifikatsiyada turlicha yondashuvlarga sabab bo‘lmoqda.

Shuningdek, sud amaliyotini bir xilda qo‘llash maqsadida qabul qilingan O‘zbekiston Respublikasi Oliy sudi Plenumining “Firibgarlik to‘g‘risidagi ishlar bo‘yicha sud amaliyoti haqida”gi qarori[2] mazkur turdagi jinoyatlarni kvalifikatsiya qilishda muhim ahamiyat kasb etadi. Mazkur hujjatda firibgarlikning obyektiv va subyektiv belgilari, aldash yoki ishonchni suiiste’mol qilish orqali mulkni egallash tushunchasi, shuningdek, jinoyat tarkibini aniqlash mezonlari batafsil yoritilgan. Biroq raqamli muhitda sodir etilayotgan kiberfiribgarlik holatlari ushbu qarorda to‘liq qamrab olinmaganligi sababli, yangi huquqiy yondashuvlarni ishlab chiqish zarurati yuzaga kelmoqda.

Amaliyotda uchrayotgan real holatlardan biri sifatida, fuqaroga telefon orqali o‘zini bank xodimi deb tanishtirgan shaxs uning plastik karta rekvizitlari va SMS-kodlarini qo‘lga kiritib, pul mablag‘larini o‘zlashtirib olgan holatni keltirish mumkin. Mazkur holatda jinoyatni kvalifikatsiya qilishda uni firibgarlik (JK 168-modda) sifatida baholash yoki axborot texnologiyalaridan foydalanib sodir etilgan jinoyat sifatida qo‘shimcha kvalifikatsiya berish masalasi yuzaga keladi. Bu esa jinoyat tarkibini aniqlashda yagona yondashuv zarurligini ko‘rsatadi.

Mazkur maqolaning maqsadi – raqamli muhitda sodir etilayotgan kiberfiribgarlik jinoyatlarining huquqiy tabiatini tahlil qilish, ularni kvalifikatsiya qilishdagi mavjud muammolarni aniqlash hamda amaldagi jinoyat qonunchiligi va sud amaliyoti asosida ularni bartaraf etish bo‘yicha ilmiy asoslangan takliflar ishlab chiqishdan iborat. Tadqiqot davomida normativ-huquqiy hujjatlar, xususan, Jinoyat kodeksi, Oliy sud Plenum qarorlari, qonun osti hujjatlar hamda statistik va amaliy materiallar kompleks ravishda tahlil qilinadi.

ASOSIY QISM

Raqamli muhitda sodir etilayotgan kiberfiribgarlik jinoyatlari jinoyat huquqi nazariyasida an’anaviy firibgarlik tarkibining zamonaviy ko‘rinishi sifatida baholanadi. O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasiga muvofiq, firibgarlik – bu aldash yoki ishonchni suiiste’mol qilish yo‘li bilan o‘zganing mulkini yoki mulkka bo‘lgan huquqini qo‘lga kiritishdan iborat jinoyat hisoblanadi. Mazkur norma umumiy ko‘rinishda barcha firibgarlik holatlarini qamrab olsada, raqamli muhitda sodir etiladigan jinoyatlarning o‘ziga xos xususiyatlari uni qo‘llashda ayrim murakkabliklarni yuzaga keltiradi.

Kiberfiribgarlikning asosiy xususiyati shundaki, unda jinoyat sodir etish vositasi sifatida axborot-kommunikatsiya texnologiyalari, jumladan internet tarmoqlari, mobil aloqa vositalari, elektron to‘lov tizimlari va dasturiy ta’minotlardan foydalaniladi. Bu esa jinoyatning obyektiv tomonini aniqlashda muhim ahamiyat kasb etadi. Ya’ni, an’anaviy firibgarlikda bevosita aloqa va aldash ustun bo‘lsa, kiberfiribgarlikda aldash masofadan turib, texnologiyalar orqali amalga oshiriladi.

Jinoyat huquqi nazariyasiga ko‘ra, firibgarlikning obyektiv tomoni uch asosiy elementdan iborat: aldash yoki ishonchni suiiste’mol qilish, mulkni egallash yoki mulkiy

huquqni qo‘lga kiritish hamda zarar yetkazish[1]. Kiberfiribgarlikda ushbu elementlar quyidagicha namoyon bo‘ladi:

✓ Aldash – soxta veb-saytlar (phishing), yolg‘on SMS yoki qo‘ng‘iroqlar orqali amalga oshiriladi;

✓ Ishonchni suiiste’mol qilish – o‘zini bank xodimi, davlat organi vakili yoki boshqa ishonchli shaxs sifatida tanishtirish orqali yuz beradi;

✓ Mulkni egallash – elektron pul mablag‘larini noqonuniy o‘tkazish, karta hisobidan yechib olish shaklida sodir etiladi.

O‘zbekiston Respublikasi Oliy sudi Plenumining “Firibgarlik to‘g‘risidagi ishlar bo‘yicha sud amaliyoti haqida”gi qarorida firibgarlik jinoyatining muhim belgilaridan biri sifatida aynan aldash yoki ishonchni suiiste’mol qilish orqali jabrlanuvchini chalg‘itish holati alohida ta’kidlangan[2]. Mazkur qarorga ko‘ra, agar shaxs o‘zganing mulkini egallash maqsadida ongli ravishda yolg‘on ma’lumot bersa yoki haqiqatni yashirsa, bu firibgarlik sifatida kvalifikatsiya qilinadi. Shu jihatdan, kiberfiribgarlikda ham aldash elementi asosiy mezon sifatida saqlanib qoladi. Biroq raqamli muhitning o‘ziga xosligi sababli jinoyat predmetining ham kengayganini ko‘rish mumkin. An’anaviy firibgarlikda moddiy buyumlar asosiy predmet bo‘lsa, kiberfiribgarlikda elektron pul mablag‘lari, bank kartalari, login-parollar, elektron hamyonlar va boshqa raqamli aktivlar jinoyat predmeti sifatida namoyon bo‘ladi. Bu esa jinoyat predmetini aniqlash va uni huquqiy jihatdan baholashda qo‘shimcha yondashuvlarni talab qiladi.

Shuningdek, kiberfiribgarlik jinoyatlarida subyektiv tomon – ya’ni ayb shakli ham muhim ahamiyatga ega. Jinoyat kodeksiga muvofiq, firibgarlik faqat to‘g‘ridan-to‘g‘ri qasd bilan sodir etiladi[4]. Ya’ni, shaxs o‘z harakatlarining ijtimoiy xavfliligini anglaydi, uning oqibatlarini oldindan ko‘ra oladi va aynan shu oqibatlarni yuzaga keltirishni istaydi. Kiberfiribgarlikda bu holat ko‘pincha oldindan rejalashtirilgan sxemalar, texnik vositalardan foydalanish va jabrlanuvchilarni maqsadli tanlash orqali namoyon bo‘ladi.

Raqamli muhitda sodir etilayotgan kiberfiribgarlik jinoyatlarini to‘g‘ri kvalifikatsiya qilish jinoyat huquqi amaliyotidagi eng murakkab masalalardan biri hisoblanadi. Amaldagi qonunchilikda firibgarlik uchun umumiy norma sifatida O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi belgilangan bo‘lsa-da, axborot texnologiyalaridan foydalangan holda sodir etilgan jinoyatlarni baholashda boshqa moddalar bilan raqobat (konkurensiya) masalasi yuzaga keladi[3]. Xususan, 168-modda bilan bir qatorda 169-modda (o‘g‘rilik), 278[6]-modda (axborot texnologiyalaridan foydalanib sodir etiladigan jinoyatlar) va ayrim hollarda 273-modda (kompyuter axborotiga ruxsatsiz kirish) normalari ham qo‘llanishi mumkin.

Kvalifikatsiyadagi asosiy muammolardan biri – jinoyat sodir etish usulini to‘g‘ri aniqlashdir. Agar shaxs jabrlanuvchini aldash yo‘li bilan uning o‘z ixtiyori bilan pul mablag‘larini o‘tkazishga undasa, bu holat firibgarlik sifatida baholanadi. Biroq, agar jinoyatchi axborot tizimiga noqonuniy kirib, mablag‘larni bevosita yechib olsa, bu holat o‘g‘rilik yoki kompyuter jinoyati sifatida kvalifikatsiya qilinishi mumkin[4]. Demak, kvalifikatsiya qilishda asosiy mezon – jabrlanuvchining xatti-harakatlari (ixtiyoriylik darajasi) va jinoyatchining ta’sir usuli hisoblanadi.

---

[1] Rustambayev, M. H. Jinoyat huquqi (Maxsus qism). Toshkent: Adolat nashriyoti, 2022, 215–230-betlar.

[2] O‘zbekiston Respublikasi Oliy sudi Plenumi. “Firibgarlik to‘g‘risidagi ishlar bo‘yicha sud amaliyoti haqida” qaror. Toshkent, 2017-yil 11-sentabr, № 24.

[3] O‘zbekiston Respublikasi Jinoyat kodeksi. Toshkent: Adolat nashriyoti, 2024.

[4] Rustambayev, M. H. Jinoyat huquqi (Maxsus qism). Toshkent: Adolat nashriyoti, 2022, 215–230-betlar.

O‘zbekiston Respublikasi Oliy sudi Plenumining tegishli qarorida firibgarlikni boshqa mulkiy jinoyatlardan farqlash mezonlari aniq belgilab berilgan[3]. Xususan, qarorga ko‘ra:

✓ agar mulk jabrlanuvchining aldangan holdagi roziligi bilan topshirilgan bo‘lsa – bu firibgarlik;

✓ agar mulk yashirin ravishda egallangan bo‘lsa – bu o‘g‘rilik;

✓ agar zo‘rlik ishlatilgan bo‘lsa – bu talonchilik yoki bosqinchilik sifatida baholanadi.

Kiberfiribgarlikda aynan “aldash” elementi asosiy rol o‘ynaganligi sababli, ko‘pchilik holatlarda u JK 168-moddasi bilan kvalifikatsiya qilinadi. Biroq amaliyotda ayrim murakkab vaziyatlar yuzaga keladi. Masalan, phishing (soxta havola) orqali foydalanuvchining karta ma’lumotlari qo‘lga kiritilib, keyinchalik uning hisobidan pul yechib olinsa, bu holatda jinoyatni faqat firibgarlik sifatida baholash yoki qo‘shimcha ravishda kompyuter axborotiga noqonuniy kirish moddalari bilan ham kvalifikatsiya qilish masalasi yuzaga keladi. Sud amaliyotida bunday holatlar bo‘yicha turli yondashuvlar mavjud. Ba’zi hollarda sudlar jinoyatni faqat firibgarlik deb baholasa, boshqa hollarda jinoyatlar yig‘indisi (konkursiya) qo‘llaniladi[4]. Bu esa yagona huquqni qo‘llash amaliyoti shakllanmaganligini ko‘rsatadi.

Yana bir muhim muammo – jinoyatni kvalifikatsiya qilishda **“yirik miqdor”** yoki **“juda yirik miqdor”** tushunchalarini aniqlashdir. Jinoyat kodeksida ushbu miqdorlar bazaviy hisoblash miqdori (BHM) asosida belgilanadi[5]. Kiberfiribgarlikda esa qisqa vaqt ichida ko‘plab jabrlanuvchilardan kichik miqdorlarda pul undirish orqali katta umumiy zarar yetkazilishi mumkin. Bu esa jinoyatni baholashda qo‘shimcha hisob-kitoblarni talab qiladi.

Shunday qilib, kiberfiribgarlikni kvalifikatsiya qilishda asosiy muammolar quyidagilardan iborat:

✓ jinoyat tarkibining to‘g‘ri aniqlanishi;

✓ turdosh jinoyatlar bilan chegaralash;

✓ jinoyatlar yig‘indisini qo‘llash masalasi;

✓ zarar miqdorini aniqlash va baholash.

Mazkur muammolarni bartaraf etish uchun qonunchilikni takomillashtirish, plenum qarorlarini yangilash hamda sud amaliyotida yagona yondashuvni shakllantirish zarur.

Raqamli muhitda sodir etilayotgan kiberfiribgarlik jinoyatlari uchun javobgarlik masalasi O‘zbekiston Respublikasi jinoyat qonunchiligida umumiy firibgarlik normalari orqali tartibga solinadi. Xususan, Jinoyat kodeksining 168-moddasida firibgarlik uchun javobgarlikning turli darajalari (oddiy, takroran, guruh bo‘lib, yirik yoki juda yirik miqdorda sodir etilgan holatlar) va ularga nisbatan qo‘llaniladigan sanksiyalar belgilangan. Mazkur modda dispozitsiyasi universalligi bilan ajralib turadi, ya’ni u an’anaviy va raqamli shakldagi firibgarlik holatlarini ham qamrab oladi.

JK 168-moddasiga muvofiq:

➢ oddiy firibgarlik uchun jarima, majburiy jamoat ishlari yoki ozodlikni cheklash jazolari qo‘llaniladi;

➢ takroran yoki bir guruh shaxslar tomonidan sodir etilgan holatlar uchun ozodlikdan mahrum qilish jazosi nazarda tutiladi;

➢ yirik va juda yirik miqdordagi firibgarliklar uchun esa uzoq muddatli ozodlikdan mahrum qilish jazosi belgilangan.

Kiberfiribgarlikda jinoyat ko‘pincha oldindan rejalashtirilgan, bir nechta shaxslar ishtirokida yoki transmilliy xarakterda sodir etilishi sababli, amaliyotda ko‘proq og‘irlashtiruvchi holatlar bilan kvalifikatsiya qilinadi. Bu esa sanksiyalarning qat’iylashuviga olib keladi.

---

[5] O‘zbekiston Respublikasi Qonuni. “To‘lovlar va to‘lov tizimlari to‘g‘risida”. 2019-yil 1-noyabr, № O‘RQ-578

O‘zbekiston Respublikasi Oliy sudi Plenumining firibgarlik bo‘yicha qarorida sudlarga jazoni individuallashtirishda jinoyatning sodir etilish usuli, zarar miqdori, aybdorning shaxsi va boshqa muhim holatlarni hisobga olish zarurligi alohida ta’kidlangan[6]. Kiberfiribgarlik holatlarida ayniqsa quyidagi omillar muhim hisoblanadi:

- ✓ jinoyatning texnologik murakkabligi;
- ✓ jabrlanuvchilar sonining ko‘pligi;
- ✓ zarar miqdorining umumiy hajmi;
- ✓ jinoyatning uyushgan guruh tomonidan sodir etilganligi.

Shu bilan birga, amaldagi qonunchilikda kiberfiribgarlik uchun alohida norma mavjud emasligi ayrim muammolarni yuzaga keltirmoqda. Ya’ni, barcha holatlar umumiy firibgarlik normasi orqali baholanmoqda. Bu esa ayrim hollarda jinoyatning haqiqiy ijtimoiy xavflilik darajasini to‘liq aks ettirmasligi mumkin.

Qonun osti hujjatlari va normativ aktlar ham mazkur sohada muhim rol o‘ynaydi. Xususan, O‘zbekiston Respublikasida “Axborotlashtirish to‘g‘risida”gi Qonun, “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonun hamda Markaziy bankning elektron to‘lovlar xavfsizligiga oid nizomlari kiberjinoyatlarning oldini olishga qaratilgan muhim huquqiy asoslarni yaratadi[7]. Ushbu hujjatlar orqali axborot xavfsizligi, shaxsiy ma’lumotlarni himoya qilish va moliyaviy operatsiyalarni amalga oshirish tartibi belgilangan.

Kiberfiribgarlikka qarshi kurashishda xalqaro tajriba ham muhim ahamiyatga ega. Ko‘plab davlatlarda mazkur turdagi jinoyatlar uchun alohida moddalar kiritilgan bo‘lib, unda axborot texnologiyalaridan foydalanish og‘irlashtiruvchi holat sifatida belgilangan. Shu nuqtai nazardan, milliy qonunchilikni takomillashtirish zarurati mavjud.

Quyidagi takliflar ilgari surilishi mumkin:

1. Jinoyat kodeksiga kiberfiribgarlik uchun alohida norma kiritish yoki 168-moddani to‘ldirish;
2. Axborot texnologiyalaridan foydalanishni og‘irlashtiruvchi holat sifatida aniq belgilash;
3. Oliy sud Plenum qarorlarini raqamli jinoyatlar xususiyatidan kelib chiqib yangilash;
4. Bank va to‘lov tizimlarida xavfsizlik choralarini kuchaytirish;
5. Aholining huquqiy va raqamli savodxonligini oshirish.

O‘zbekiston Respublikasi Ichki ishlar vazirligi va ochiq manbalarda e’lon qilingan ma’lumotlarga ko‘ra, 2021–2024 yillar davomida firibgarlik jinoyatlarining umumiy soni hamda ularning tarkibida kiberfiribgarlik ulushi quyidagi dinamikani ko‘rsatgan:

2021-yil: jami firibgarlik jinoyatlari soni taxminan 18 000 tani tashkil etgan bo‘lib, shundan 15–18 % (taxminan 2 700–3 200 ta holat) axborot texnologiyalari orqali sodir etilgan;

2022-yil: umumiy ko‘rsatkich 22 000 taga yetgan, kiberfiribgarlik ulushi 22–25 % (taxminan 5 000 ta holat);

2023-yil: firibgarlik jinoyatlari soni 27 000 dan oshgan bo‘lib, ularning 30–35 % (8 000 dan ortiq holat) raqamli muhitga to‘g‘ri kelgan;

---

[6] O‘zbekiston Respublikasi Oliy sudi Plenumi. “Firibgarlik to‘g‘risidagi ishlar bo‘yicha sud amaliyoti haqida” qaror. Toshkent, 2017-yil 11-sentabr, № 24.

[7] O‘zbekiston Respublikasi Oliy sudi Plenumi. “Firibgarlik to‘g‘risidagi ishlar bo‘yicha sud amaliyoti haqida” qaror. Toshkent, 2017-yil 11-sentabr, № 24.

2024-yil: dastlabki ma’lumotlarga ko‘ra, umumiy firibgarlik jinoyatlari 30 000 taga yaqinlashgan va ularning 38–42 % (11 000–12 500 ta holat) aynan kiberfiribgarlik sifatida qayd etilgan.[8]

Mazkur statistik ko‘rsatkichlar shuni anglatadiki, so‘nggi to‘rt yil ichida kiberfiribgarlikning umumiy firibgarlik tarkibidagi ulushi deyarli 2,5 barobarga oshgan. Bu esa raqamli texnologiyalarning kengayishi bilan bir qatorda, jinoyatchilar tomonidan yangi usullarning faol qo‘llanilayotganini ko‘rsatadi.

Kiberfiribgarlikning eng keng tarqalgan shakllari ham statistik jihatdan aniqlangan. 2024-yil ma’lumotlariga ko‘ra:

✓ bank kartalari bilan bog‘liq firibgarliklar – 60–65 %;
✓ telefon orqali (o‘zini bank yoki tashkilot xodimi sifatida tanishtirish) – 20–25 %;
✓ phishing (soxta sayt va havolalar orqali) – 10–12 %;
✓ boshqa usullar (ijtimoiy tarmoqlar, onlayn savdo firibgarligi) – 5–8 % ni tashkil etgan.[9]

Zarar miqdori bo‘yicha tahlil shuni ko‘rsatadiki, 2023-yilda kiberfiribgarlik natijasida yetkazilgan umumiy moddiy zarar 300 mlrd so‘mdan ortiq bo‘lgan bo‘lsa, 2024-yilda bu ko‘rsatkich 500 mlrd so‘mga yaqinlashgan. Bu esa nafaqat jinoyatlar soni, balki ularning iqtisodiy xavflilik darajasi ham ortib borayotganini anglatadi.

Hududlar kesimida tahlil qilinganda, kiberfiribgarlik jinoyatlari asosan yirik shaharlarda yuqori ko‘rsatkichga ega:

Toshkent shahri – 35–40 %;
Toshkent viloyati – 10–12 %;
Samarqand va Farg‘ona viloyatlari – har biri 7–9 %;
boshqa hududlar – 30 % atrofida.[10]

Bu holat urbanizatsiya darajasi va raqamli xizmatlardan foydalanish intensivligi bilan bevosita bog‘liq.

Shuningdek, jinoyatlarning ochilish darajasi (ochilgan jinoyatlar ulushi) ham muhim ko‘rsatkich hisoblanadi. 2024-yil yakunlariga ko‘ra:

✓ an’anaviy firibgarlik jinoyatlarining ochilish darajasi – 85–90 %;
✓ kiberfiribgarlik bo‘yicha esa bu ko‘rsatkich atigi 60–70 % ni tashkil etgan.[11]

Bu esa kiberjinoyatlarni fosh etish murakkabroq ekanini, texnik va protsessual qiyinchiliklar mavjudligini ko‘rsatadi.

Yosh tarkibi bo‘yicha tahlil natijalari ham qiziqarli: kiberfiribgarlik jinoyatlarini sodir etgan shaxslarning asosiy qismi 18–35 yosh oralig‘iga to‘g‘ri keladi (taxminan 70 %), bu esa ularning axborot texnologiyalaridan faol foydalanishi bilan izohlanadi[12].

Statistik ma’lumotlar kiberfiribgarlik jinoyatlarining keskin o‘sish tendensiyasini, ularning iqtisodiy zararining ortib borayotganini va jinoyat tarkibida muhim o‘rin

---

[8] O‘zbekiston Respublikasi Ichki ishlar vazirligi. Jinoyatchilik statistikasi bo‘yicha yillik hisobot (2021–2024). Toshkent, 2024.

[9] O‘zbekiston Respublikasi Markaziy banki. Elektron to‘lov tizimlari va moliyaviy xavfsizlik bo‘yicha yillik hisobot. Toshkent, 2024.

[10] O‘zbekiston Respublikasi Ichki ishlar vazirligi. Jinoyatchilik statistikasi bo‘yicha yillik hisobot (2021–2024). Toshkent, 2024.

[11] O‘zbekiston Respublikasi Bosh prokuraturasi. Kiberjinoyatlar bo‘yicha tahliliy ma’lumotlar to‘plami. Toshkent, 2024.

[12] Kriminologik tadqiqotlar instituti. Raqamli jinoyatchilik va kiberfiribgarlik bo‘yicha ilmiy tahlil. Toshkent, 2023, 45–68-betlar.

egallayotganini yaqqol ko‘rsatadi. Bu esa jinoyat huquqi siyosatini qayta ko‘rib chiqish, profilaktika choralarini kuchaytirish hamda huquqni qo‘llash amaliyotini takomillashtirish zarurligini asoslaydi.

XULOSA

Raqamli muhitda kiberfiribgarlik jinoyatlarining tahlilim natijasi shuni ko‘rsatadiki, ushbu turdagi jinoyatlar bugungi kunda nafaqat O‘zbekiston Respublikasi, balki butun dunyo jinoyat huquqi tizimi oldida turgan eng dolzarb muammolardan biri hisoblanadi. Tadqiqot davomida aniqlanishicha, kiberfiribgarlik o‘zining huquqiy tabiati jihatidan Jinoyat kodeksining 168-moddasi bilan qamrab olingan firibgarlikning zamonaviy ko‘rinishi bo‘lib, u an’anaviy usullardan farqli ravishda axborot-kommunikatsiya texnologiyalari orqali amalga oshiriladi. Tahlillar natijasida kiberfiribgarlik jinoyatlarining kvalifikatsiya qilish jarayonida bir qator muammolar mavjudligi aniqlandi. Xususan, jinoyatni turdosh tarkiblardan ajratish (o‘g‘rilik, kompyuter jinoyatlari), jinoyatlar yig‘indisini to‘g‘ri qo‘llash, shuningdek, zarar miqdorini aniqlashdagi murakkabliklar amaliyotda yagona yondashuv shakllanmaganligini ko‘rsatadi. O‘zbekiston Respublikasi Oliy sudi Plenum qarorlari ushbu yo‘nalishda muhim yo‘l-yo‘riq bo‘lsa-da, raqamli jinoyatlar xususiyatlari to‘liq qamrab olinmaganligi sababli huquqni qo‘llash amaliyotida ayrim ziddiyatlar saqlanib qolmoqda[13].

Statistik tahlillar esa kiberfiribgarlik jinoyatlarining keskin o‘sish tendensiyasini tasdiqladi. 2021–2024 yillar oralig‘ida ushbu jinoyatlarning ulushi sezilarli darajada oshib, firibgarlik jinoyatlarining qariyb yarmiga yaqin qismini tashkil etish darajasiga yetgan. Bu esa raqamli texnologiyalarning kengayishi bilan birga jinoyatchilikning ham yangi shaklga o‘tganini anglatadi. Ayniqsa, bank kartalari va onlayn to‘lov tizimlari orqali sodir etilayotgan firibgarliklar eng keng tarqalgan ko‘rinish sifatida ajralib turadi. Shuningdek, kiberfiribgarlik natijasida yetkazilayotgan moddiy zarar hajmining ortib borishi va jinoyatlarning ochilish darajasi an’anaviy firibgarlikka nisbatan pastligi ushbu sohada huquqni muhofaza qiluvchi organlar uchun qo‘shimcha qiyinchiliklar tug‘dirayotganini ko‘rsatadi. Bu holat texnik bazani mustahkamlash, kadrlar malakasini oshirish hamda xalqaro hamkorlikni kengaytirish zarurligini asoslaydi.

Tadqiqot natijalarim asosida quyidagi xulosalarga keldim:

✓ kiberfiribgarlik jinoyatlarini alohida tarkib sifatida normativ jihatdan takomillashtirish zarur;

✓ Jinoyat kodeksida axborot texnologiyalaridan foydalanishni og‘irlashtiruvchi holat sifatida aniq belgilash lozim;

✓ Oliy sud Plenum qarorlarini raqamli jinoyatlar xususiyatiga mos ravishda yangilash maqsadga muvofiq;

✓ bank va to‘lov tizimlarida xavfsizlik standartlarini kuchaytirish hamda profilaktika choralarini kengaytirish zarur.

Umuman olganda, kiberfiribgarlik jinoyatlarining ortib borishi jinoyat huquqi tizimidan tezkor moslashuvchanlikni, qonunchilikning esa raqamli transformatsiyaga mos ravishda doimiy takomillashtirilishini talab etadi. Mazkur yo‘nalishda samarali huquqiy mexanizmlarni ishlab chiqish jamiyatning iqtisodiy xavfsizligini ta’minlashda muhim ahamiyat kasb etadi.

[13]O‘zbekiston Respublikasi Oliy sudi Plenumi. “Firibgarlik to‘g‘risidagi ishlar bo‘yicha sud amaliyoti haqida” qaror. Toshkent, 2017-yil 11-sentabr, № 24

FOYDALANILGAN MANBALAR

1. O‘zbekiston Respublikasi Jinoyat kodeksi. Toshkent: Adolat nashriyoti, 2024. https://lex.uz/docs/111453
2. O‘zbekiston Respublikasi Oliy sudi Plenumi. “Firibgarlik to‘g‘risidagi ishlar bo‘yicha sud amaliyoti haqida” qaror. Toshkent, 2017-yil 11-sentabr, № 24. https://lex.uz
3. O‘zbekiston Respublikasi Qonuni. “Axborotlashtirish to‘g‘risida”. 2003-yil 11-dekabr, № 560-II. https://lex.uz/docs/8452
4. O‘zbekiston Respublikasi Qonuni. “To‘lovlar va to‘lov tizimlari to‘g‘risida”. 2019-yil 1-noyabr, № O‘RQ-578.https://lex.uz/docs/4548608
5. O‘zbekiston Respublikasi Markaziy banki. Elektron to‘lov tizimlari va moliyaviy xavfsizlik bo‘yicha yillik hisobot. Toshkent, 2024. https://cbu.uz
6. O‘zbekiston Respublikasi Ichki ishlar vazirligi. Jinoyatchilik statistikasi bo‘yicha yillik hisobot (2021–2024). Toshkent, 2024. https://iiv.uz
7. O‘zbekiston Respublikasi Bosh prokuraturasi. Kiberjinoyatlar bo‘yicha tahliliy ma’lumotlar to‘plami. Toshkent, 2024. https://prokuratura.uz
8. Rustambayev, M. H. Jinoyat huquqi (Maxsus qism). Toshkent: Adolat nashriyoti, 2022, 215–230-betlar.
9. Kriminologik tadqiqotlar instituti. Raqamli jinoyatchilik va kiberfiribgarlik bo‘yicha ilmiy tahlil. Toshkent, 2023, 45–68-betlar.