



## Bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyatlarining kriminalistik tavsifi

*Amirxon Nosirov Bahodir o‘g‘li*

*Toshkent davlat yuridik universiteti*

*“Jinoyat qonunchiligini qo‘llash nazariyasi va amaliyoti” soha mutaxassisligi magistri*

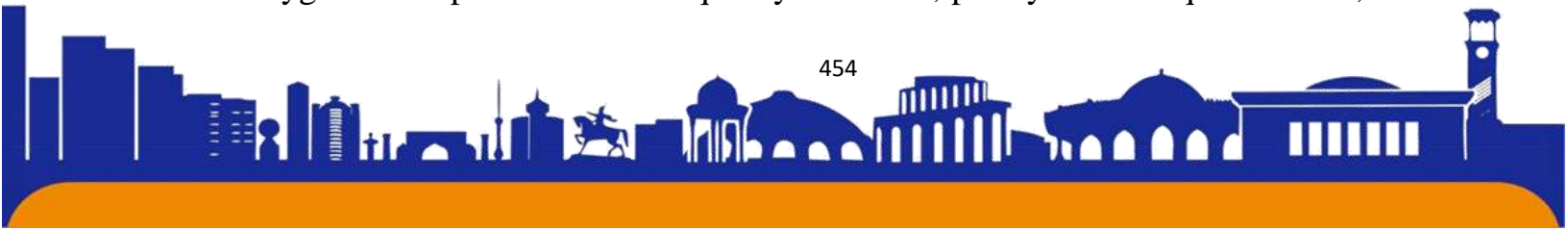
**Annotatsiya:** Ushbu maqolada bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyatining umumiy tushunchasi va kriminalistik tahlili bayon etilgan. Unda bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyatining kriminalistik tavsif elementlari, ya‘ni jinoyat predmeti, jinoyat sodir etish usullari, jinoyat izlari, jinoyatchining shaxsi haqidagi ma‘lumotlar, jinoyat shart-sharoitlari yoritilgan.

Shu bilan birga, bank kartalari bilan bog‘liq firibgarlik jinoyatini tergov qilishda raqamli izlar bilan ishlash jarayoni, milliy qonunchilik va huquqni qo‘llash amaliyotida yuzaga kelayotgan muammolar hamda bo‘shliqlar tanqidiy ko‘rib chiqilgan. Ularni bartaraf etishning ilmiy asoslangan yo‘llari va mezonlari ishlab chiqilgan. Maqola raqamli izlar bilan ishlash sohasida amalga oshirilgan ilmiy-amaliy tadqiqotlar, nazariyotchi olimlar hamda amaliyotchi xodimlar fikr-mulohazalari asosida tayyorlangan.

Bundan tashqari, onlayn jinoyat turlaridan biri bo‘lmish internet tovlamachilik jinoyatini bank kartalari bilan bog‘liq firibgarlik jinoyatiga o‘xshash jihatlari muhokama qilingan. Maqolada sohada yuzaga kelayotgan muammolar tizimli, huquqiy, ilmiy-amaliy jihatdan tahlil etilgan, bu yuzasidan mualliflik xulosalari shakllantirilgan. Qonun chiqaruvchi va uni qo‘llovchi subektlar uchun ilmiy asoslangan taklif hamda tavsiyalar ishlab chiqilgan.

**Kalit so‘zlar:** bank kartalari, bank kartalari bilan bog‘liq firibgarlik jinoyatlari, jinoyat izlari, jinoyat usuli, jinoyatchi shaxsi, elektron to‘lov tizimlari.

**Kirish.** Bugungi kunda raqamli texnologiyalar kundan kunga taraqqiy etib, oddiygina bank plastik kartasi orqali oylik maosh, pensiya va nafaqalarni olish, kredit





olish va to'lash, kamunal to'lovlarni amalga oshirish, soliq va boshqa turli xil to'lovlarni hech qanday qiyinchiliklarsiz amalga oshirish mumkin. Mamlakatdagi raqamlashtirish jarayonlari hamda onlayn xizmatlar bozoridagi talab va taklifni ortib borishi bank kartalarini qulay to'lov tizimiga aylanishiga olib keldi. Natijada, naqt to'lovlarsiz moliyaviy hisob-kitoblarni amalga oshirish kundalik ehtiyojlarni qondirishning ajralmas qismiga aylanib ulgurdi. Ayni damda bu to'lov tizimlari insonlar nigohida qanchalar mukammal va universal bo'lib tuyulsada, afsuski hozircha bu tizimni ham nuqson va kamchiliklardan to'la xoli va xavsiz deb bo'lmaydi.

Global axborot almashinuvi asrida sun'iy intellekt va raqamli texnologiyalarni takomillashtirilishi axborot xavfsizligi bilan bog'liq turli muammolarni yuzaga keltirmoqda. Bunga asosiy sabab sohada kiberjinoyatchilikning avj olishi hamda unga qarshi kurashning uslubiy ta'minotlarini ishlab chiqilmaganligi bilan bog'lash mumkin.

Jinoiy maqsadni amalga oshirishda kompyuter texnikasidan asosiy vosita yoki quroli sifatida foydalanish kundan-kunga ommalashib bormoqda. Kompyuter texnikasini mehnat munosabatlarining asosiy vositasiga aylanishi va ma'lumotmotlar bazalari bilan samarali ishlash imkonini berishi moliyaviy xizmatlar ko'rsatish sohasida inqilobiy o'zgarishlarga olib kelmoqda. Xususan, bugun iqtisodiyot sohasida moliyaviy xizmatlar ko'rsatishning turli shakllarini joriy etilishi bu borada bank plastik kartlari bilan bog'liq kiberjinoyatlarni o'sishi uchun ham zamin yaratmoqda.

Mulk huquqining daxlsizligi konstitutsiyaviy norma darajasida mustahkamlangan bo'lib, unga har qanday tahdid, avvalo, konstitutsiyaviy normaning buzilishini anglatadi. Shu nuqtai nazardan qaralganda, bank kartalaridan foydalanish bilan bog'liq firibgarlik jinoyati o'zgarar mulkini talon-toroj qilish bilan bog'liq boshqa jinoyatlardan ijtimoiy xavfi yuqoriligi bilan farq qiladi.

2022 yil 28 yanvardagi O'zbekiston Respublikasi Prezidentining "Yangi O'zbekistonning 2022–2026 yillarga mo'ljallangan taraqqiyot strategiyasi to'g'risida"gi PF–60-son Farmoni (keyingi o'rinlarda Farmon deb yuritiladi) bilan tergov faoliyatini nazorat qilish, axborot texnologiyalaridan foydalangan holda sodir etilayotgan yangi turdagi jinoyatlar, shu jumladan kiberjinoyatlarni fosh etish bo'yicha tezkor-qidiruv faoliyatini isloh qilish, qo'shimcha kuch va vositalarni jalb qilish hamda ushbu jinoyatlarga qarshi kurashish jarayonlarida fuqarolarning qadr-qimmatini va





erkinligini himoya qilishning samaradorligini yanada oshirish bo'yicha qator vazifalar belgilandi<sup>1</sup>.

Farmonga binoan «2023–2026 yillarga mo'ljallangan O'zbekiston Respublikasining kiberxavfsizlik strategiyasi»ni ishlab chiqish vazifasi qo'yildi.

Bunda, kiberjinoatchilik uchun jinoiy javobgarlikni qayta ko'rib chiqish, axborot maydonidagi kiberhujum va tahdidlarni monitoring qilish tizimini yanada takomillashtirish, xususan, kiberxavfsizlikning yagona tarmog'ining texnik infratuzilmasini kengaytirish vazifalari belgilab olindi.

Firibgarlar tomonidan bank kartalaridan pul yechib olishning yangidan-yangi usul va vositalarini qo'llashi jinoyat mexanizmlarini murakkablashuviga olib kelmoqda. Statistik ma'lumotlarga tayanib shuni aytish mumkinki, O'zbekistonda firibgarlik so'nggi 4 yilda 4 baravarga, ya'ni 2018 yilda 6 483 ta, 2019 yilda 6 321 ta, 2020 yilda 10 496 ta, 2021 yilda 24 554 taga, kiberfiribgarlik esa so'nggi 3 yilda 8,3 baravarga ko'payib, hozirda umumiy jinoyatchilikning qariyb 5 foiziga yetgan<sup>2</sup>.

“Kompyuter firibgarligi” (**computer fraud**) atamasi, o'tgan asrning 70-yillarida paydo bo'lgan<sup>3</sup> bulib, hozirgi kunga qadar olimlar tomonidan bir qancha bahs munozalarga sabab bo'lmoqda. Xususan, D.A Zakirova kompyuter firibgarligi bu “kompyuter texnikasi yordamida aldash yoki ishonchni suiiste'mol qilish yo'li bilan o'zganing mulkini yoki o'zganing mulkiga bo'lgan huquqni qo'lga kiritish” degan tushunchani ilgari suradi<sup>4</sup>. M.A. Yefremova esa, kiberfiribgarlik va kompyuter firibgarligi bir xil tushuncha, ya'ni sinonimlar deb hisoblaydi<sup>5</sup>. Professor N.Lopashenko, kompyuter firibgarligini naqd bo'lmagan pul mablag'larini va nodokumentar qimmatli qog'ozlarni qo'lga kiritish uchun kompyuter texnologiyalaridan foydalanish bilan bog'liq firibgarlik deb tariflaydi<sup>6</sup>.

<sup>1</sup> 2022 йил 28 январдаги Ўзбекистон Республикаси Президентининг «Янги Ўзбекистоннинг 2022–2026 йилларга мўлжалланган тараққиёт стратегияси тўғрисида»ги ПФ–60-сон Фармони.

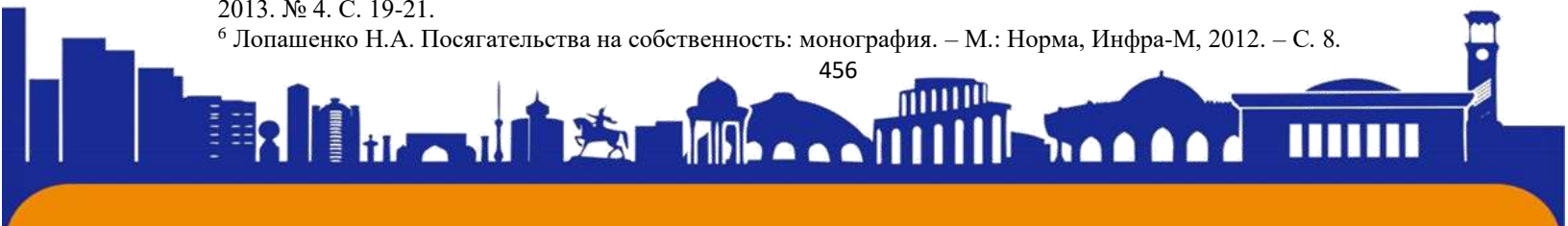
<sup>2</sup> <https://stat.uz/uz/rasmiy-statistika/crime-and-justice-2>

<sup>3</sup> Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет. Дисс. на соис. уч. степ. канд. юрид. наук. – Пятигорск, 2010. – С. 24.

<sup>4</sup> Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества. Владимир, 2002. – 211 с.

<sup>5</sup> Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. № 4. С. 19-21.

<sup>6</sup> Лопашенко Н.А. Посягательства на собственность: монография. – М.: Норма, Инфра-М, 2012. – С. 8.





Bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyati fosh etilishi juda qiyin bo‘lgan jinoyatlardan biri bo‘lib, puxta rejalashtirilganligi, o‘ta murakkabligi hamda transchegaraviy xususiyatga egaligi bilan boshqa turdagi jinoyatlardan farq qiladi. Ushbu jinoyat tushunchasi ba‘zi kriminalistik adabiyotlarda onlayn firibgarlik, kiberfiribgarlik deb keltirilgan bo‘lsa, ba‘zilarida esa kompyuter firibgarligi deb keltiriladi.

Qonunchiligimizda onlayn firibgarlik, kiberfiribgarlik, bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyati tushunchalari hali to‘liq va batafsil yoritilmagan. Hozirda bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyatini sodir etish holati va usuliga qarab, O‘zbekiston Respublikasi Jinoyat kodeksining **168-moddasi 2-qismi “v”** bandiga asosan **kompyuter texnikasi vositalaridan foydalanib** sodir etilganda ushbu norma bilan kvalifikatsiya qilinadi.

Bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyatining kriminalistik tavsifi ham kriminalistika nazariyasining umumiy qonuniyatlaridan chetga chiqmaydi. Biroq, uning strukturasi elementlar o‘ziga xosligi bilan ajrab turadi.

### **MUHOKAMA VA NATIJALAR**

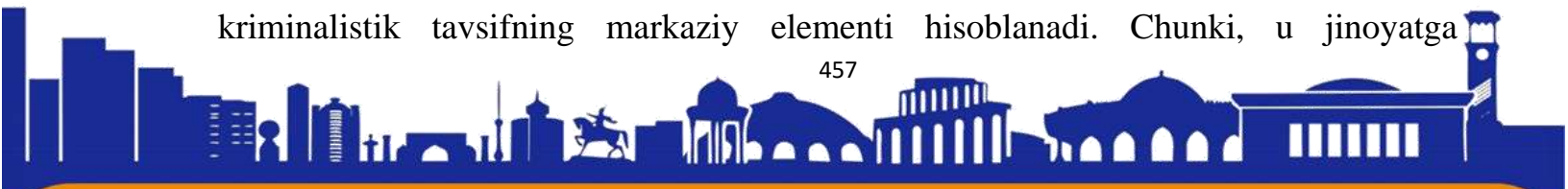
Ushbu jinoyatining kriminalistik tavsifi tarkibiy elementlari quydagilardan iborat:

- jinoiy tajovuz predmeti;
- jinoyat sodir etish usullari;
- jinoyat izlari;
- shart-sharoitlar (vaqti, joyi va boshqa holatlar);
- jinoyatchining shaxsi haqidagi ma’lumotlar.

#### **Jinoiy tajovuz predmeti**

Odatda pul, qimmatbaho buyumlar, texnika va boshqa ashyolar firibgarlik jinoyatining predmeti bo‘ladi. Ammo, bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyatining bevosita predmeti bu o‘zganing mulki, ya’ni o‘zgalarning bank karta hisob raqamlarida saqlanayotgan pulidir. Biroq, to‘g‘ridan-to‘g‘ri bank kartasining o‘zi jinoyat predmeni bo‘la olmaydi, chunki jinoyatchining motiv-maqsadi faqatgina karta hisob raqamlarida saqlanayotgan pulni jabrlanuvchini aldash va ishonchini suiiste’mol qilish yo‘li bilan qo‘lga kiritish hisoblanadi.

Bank kartalari bilan bog‘liq firibgarlik jinoyatlarini sodir etishning usuli kriminalistik tavsifning markaziy elementi hisoblanadi. Chunki, u jinoyatga



tayyorgarlik ko‘rish, amalga oshirish va jinoyatni yashirish bo‘yicha jinoyatchilarning harakatlarini yagona maqsadda birlashtiradi.

Bank kartalari bilan bog‘liq firibgarlik jinoyatini sodir etishning bir necha xil usullari mavjud. Xususan, amaliyotda keng tarqalganlar usullardan biri bu – internet va mobil aloqa vositalari orqali sodir etiladigan firibgarlikdir. Jinoyatchilar jinoiy qilmishni sodir etish vositasi sifatida internet, kompyuter va mobil qurilmalardan foydalanishadi.

### **Jinoyat sodir etish usullari**

#### ***Fishing***

Bank kartalari bilan bog‘liq firibgarlik jinoyatini sodir etish usullaridan biri bu “fishing” ya’ni “baliq ovi” usulidir. Bunda IT texnologiya sohasida yetarli bilim va ko‘nikmalarga ega firibgarlar tomonidan foydalanuvchining ishonchiga kirib, bank kartasiga doir maxfiy ma’lumotlari egallanadi<sup>7</sup>.

Jinoyatni sodir etish usulining o‘ziga xos xususiyati shundaki, jinoyatchi tomonidan masofadan turib aloqa vositalari yoxud sohta veb-sahifalar orqali foydalanuvchining ijtimoiy tarmog‘idagi akkaunti, elektron pochta yoki uyali aloqa vositalariga sms habar yuboriladi. Bunda ijtimoiy muhandislik usullaridan foydalaniladi. Bu xususida quyida batafsil tushuntirish keltirib o‘tamiz.

“Fishing” bilan shug‘ullanuvchi jinoiy guruhlar jabrlanuvchidan shaxsiy ma’lumotlarini kiritishni so‘rab turli shaklda xabarnoma jo‘natishadi. Jabrlanuvchi bank xizmatlaridan foydalanish uchun bankning rasmiy veb-saytiga kirayotganliklariga ishonadi. Biroq, firibgarlar tomonidan yaratilgan tuzoqlarga laqqa tushadilar. Xususan, soxta saytga ism-sharifi, karta rekvizitlari, pin kodi kiritish orqali o‘zlari bilmagan holda “fishing”chilar qarmog‘iga ilinishadi<sup>8</sup>. Soxta saytlar yaratish bu zamonaviy fishing uslublaridan biridir. Bunday fishing saytlarini maxsus bilim va ko‘nikmalarsiz aniqlash juda mushkul.

#### ***Vishing***

---

<sup>7</sup> Shazzo S.K. Sposobi soversheniya moshennichestva v otnoshenii grajdan [Methods of committing fraud against citizens]. Vestnik Adigeyskogo gosudarstvennogo universiteta. Seriya 1: Yurisprudentsiya. 2008. № 2. S. 5.

<sup>8</sup> Izotov D. S., Bikova N. N. Vidi moshennichestva s bankovskimi kartami [See bank card fraud]. Vestnik NGIEI. 2015.



Hozirgi kunda yurtimizda yeng kup kuzatilayotgan firibgarlik usulidan biri bu vishing onlayn firibgarligidir. Firibgarlikning bu usulida firibgarlar o‘z “o‘ljalarini” telefon orqali qo‘lga kiritishadi. Vishing so‘zi ingliz tilidan ya’ni, “voice” ovoz va “fishing” baliq ovi so‘zlarining jamlanmasidan hosil bo‘lgan<sup>9</sup>. Yuqoridagi firibgarlik usulida firibgarlar uzini bank xodimi, to‘lov tizimi xodimi, yoki shunga o‘xshash har xil yolg‘on va uydirmalar orqali jabrlanuvchilardan ularga jo‘natilgan maxfiy sms malumotlarini olishadi.

Mamlakatimizda ushbu holatlar keskin ko‘payib, xususan firibgarlar tomonidan o‘zini “Click yoki boshqa bir to‘lov tizimi xodimi” deb tanishtirib, fuqarolarni alash va ishonchiga kirish orqali go‘yoki tizimdagi ayrim kamchiliklarni tuzatish hamda to‘lov bilan bog‘liq kamchiliklarni bartaraf etish niqobida jabrlanuvchiga sms jo‘natib, undan sms raqamini aytishini so‘rashyapti. SMS raqami aytilishi bilan pul mablag‘lari turli plastik kartalar yoki telefon raqamlarga tranzaksiya qilinib, Click orqali Qiwi hamyonga o‘tkaziladi va jinoiy yo‘l bilan undirilgan pul mablag‘lari (so‘m) xorijiy valyutga konvertatsiya qilinadi.

### ***Meros firibgarligi***

Jabrlanuvchi nomiga chet eldagi qarindoshidan katta miqdordagi meros qoldirilgani haqidagi habar go‘yoki uning advokati niqobida beriladi. Shundan so‘ng, pasport hamda plastik karta raqamlariga doir mahfiy ma‘lumotlar merosni rasmiylashtirish hamda dastlabki to‘lovlarni amalga oshirish uchun aldov yo‘li bilan olib qo‘yiladi.

### ***Xalqaro pochta jo‘natmalari***

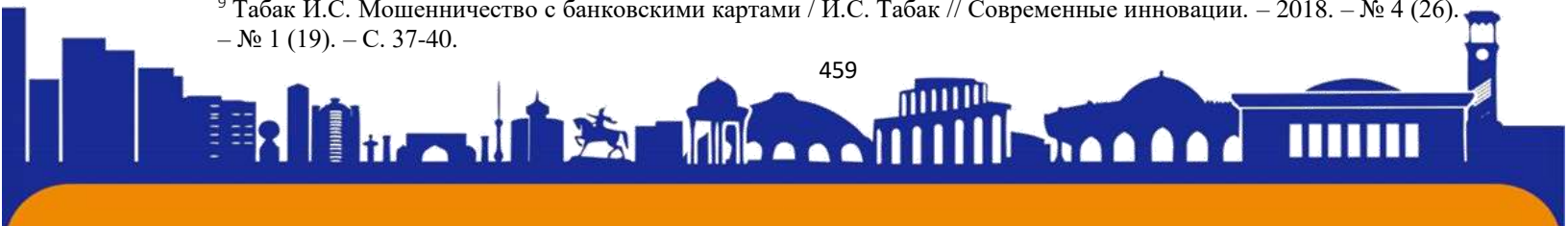
Jabrlanuvchiga ma‘lum turdagi qimmatbaho yuk yuborilgani, qabul qilib olish uchun pochta chiqimlarini to‘lash bo‘yicha turli xil pochta jo‘natmalari yorlig‘i yoxud jo‘natma uning nomiga ekanligini tasdiqlovchi fotosuratlar jo‘natiladi. Shu orqali plastik karta raqamiga doir mahfiy ma‘lumotlar aldov yo‘li bilan olinadi.

### ***Fishing tanlovlar***

Ijtimoiy tarmoqlarda soxta tanlovlar tashkil qilish. Bu xolatda yutuq sifatida avtotransport vositasi yoki oxirgi rusumli telefon apparati qo‘yiladi. E’tiborli jihati shundaki, tashkilotchilar deyarli barcha ishtirokchilarni “Siz lotoreyada g‘olib

---

<sup>9</sup> Табак И.С. Мошенничество с банковскими картами / И.С. Табак // Современные инновации. – 2018. – № 4 (26). – № 1 (19). – С. 37-40.





chiqdingiz yoki sovg‘alar soni cheklangan aksiyada ishtirok eting, sovg‘ani qo‘lga kiriting” kabi yutuq bilan tabriklab yoxud tanlovda ishtirok etishi uchun qiziqtirib habar jo‘natishadi. Odatda, fishing tanlovi ishtirokchilari tanlovda bir necha marotaba ishtirok etganidan so‘ng ushbu jarayon firibgarlik ekanligiga tushunib yetishadi.

### ***Internet-tilanchilik – soxta xayriya jamg‘armalari***

Internet sahifalar hamda ijtimoiy tarmoqlarda turli xil kasallikka chalingan yoxud og‘ir ahvoldagi shaxslarni fotosuratlarini joylashtirib ularning nomidan moddiy yordam so‘rash. Firibgarlar ko‘proq insoniylik, rahm-shavqat va ishonuvchanlik his tuyg‘ularini uyg‘otuvchi psixologik ta’sir etish usullariga e’tibor qaratishadi. Odatda, nomi e’lon qilinayotgan shaxslar ular uchun pul mablag‘lari jamg‘arilayotgani haqida hech qanday ma’lumotga ega bo‘lishmaydi. Sababi, ehson qilingan har qanday pul mablag‘lari to‘g‘ridan-to‘g‘ri firibgarlarning hisobraqamlariga o‘tkaziladi.

### ***Internet do‘konlar bilan bog‘liq firibgarliklar***

Bazi firibgarlar qalbaki, sifatsiz tovarlar yoki maxsulotlar savdosi bilan shug‘ullanib xaridorlarni chuv tushursa, boshqalari maxsulot uchun oldindan qisman yoki to‘liq to‘lov qilishni talab qiladi<sup>10</sup>. To‘lov amalga oshirilgach xaridorga tovar yetkazilmaydi.

So‘nggi yillarda internet do‘konlari bilan bog‘liq firibgarlik mamlakatimiz hududida ham o‘sib borayotganligi kuzatilmoqda. Xususan, hozirda “OLX.uz” onlayn platformasi orqali amalga oshirilayotgan savdolarda bank plastik kartalaridan pul mablag‘larini yechib olinishi bilan bog‘liq holatlar mavjud.

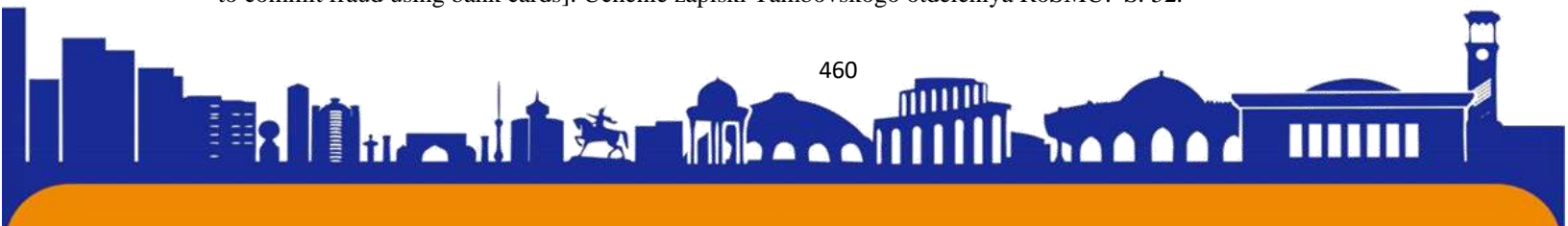
Firibgarlar jabrlanuvchiga boshqa viloyatda yoki xorijda ekanligini vaj qilib, undan sotib olinishi rejalashtirilgan tovarga to‘lov qilish uchun bank karta raqami va yuborilgan smsni aytishni aldov yo‘li bilan so‘rab olishadi. Shundan so‘ng, yuqorida ko‘rsatilgan protsedura bo‘yicha ishlar amalga oshiriladi.

### ***Nikoh firibgarligi***

Ijtimoiy tarmoqdagi o‘zga shaxslarga doir fotosuratlaridan foydalanib, ularning nomidan jabrlanuvchilar bilan yozishmalar olib boriladi va ishonchiga kiradi. Vaqt

---

<sup>10</sup> Kozodaeva O. N., Obidenova A. S. Sposobi soversheniya moshennichestva sispol’zovaniem bankovskix kart [Ways to commit fraud using bank cards]. Uchenie zapiski Tambovskogo otdeleniya RoSMU. S. 52.



o'tishi bilan jabrlanuvchilardan moddiy yordam so'rab, ko'zlangan mablag'ni qo'lga kiritganidan so'ng akkaunt o'chirib yuboriladi.

### ***Frilanserlik xizmatlari***

Frilanserlik xizmati – kelishilgan xizmat evaziga buyurtmachiga sayt yaratish, maqola yozish, tarjima ishlari, reklama logotiplari, video meyerlik va boshqa shakldagi onlayn xizmatlarni ko'rsitishdir.

Ushbu usul mohiyati jabrlanuvchi (frilanser) buyurtmachiga (firibgar) buyurtmani jo'natish bilan jinoyatchi kelishilgan pulni to'lamasdan g'oyib bo'lishida namoyon bo'ladi.

Mamlakatimizda kuzatilayotgan onlayn jinoyat turlaridan yana biri bu ***internet tovlamachilik*** bo'lib, quydagi vaziyat bunga yorqin misol tariqasida keltirilishi mumkin.

Jinoyatchilar internet tarmog'idagi pornografik materiallar, shavqatsizlikni targ'ib qiluvchi saytlarda o'zlarini huquqni muhofaza qiluvchi organlar yoxud IIV Kiberxavfsizlikga qarshi kurash bo'limi tomonidan foydalanuvchi ma'muriy javobgarlikka tortilgani va ma'lum bir pul miqdorini belgilangan hisob raqamga ko'chirishi shartligini talab qilishadi. *Masalan, "O'zbekiston Respublikasi IIV Kiberjinoyatlarga qarshi kurash bo'limidan bildirishnoma! Siz O'zbekiston Respublikasi qonunchiligi bilan taqiqlangan materiallar, ya'ni pedofiliya, zo'ravonlikni targ'ib qilish elementlariga ega bo'lgan pornografiya materiallari mavjud bo'lgan pornografik saytlarga tashrif buyurganligingiz uchun blokirovka qilindingiz. Blokirovkani yechish uchun Siz shu plastik hisobraqamiga yoki davlat hamyoniga 310.000 so'm miqdorida jarima to'lashingiz zarur"*<sup>11</sup>.

Odatda, bunday noqulay vaziyatdan tezroq chiqish hamda sharmandalik va javobgarlikdan qutulish maqsadida talab qilingan pul summasini tegishli hisob raqamga o'tkaziladi. Biroq, afsuski IIV Kiberjinoyatlarga qarshi kurash bo'limi xech kimga bunday habar yubormaydi...

Ushbu holat o'zida firibgarlik alomatlarini ham mujassamlashtirgan bo'lib, bu vaziyatda biz onlayn firibgarlik va onlayn tovlamachilik tushunchalarini bir biridan ajratib olishimiz lozim. Sababi, ***birinchidan***, jinoyatchi o'zini huquqni muhofaza

---

<sup>11</sup> <https://iiv.uz/news/ogoh-boling-internet-tarmogida-firibgarlar>





qiluvchi organ hodimi deb tanishtirib, jabrlanuvchini aldaydi. ***Ikkinchidan***, jinoyatchi jabrlanuvchining internet tarmog‘idan foydalanish huquqini muayyan vaqt oralig‘ida cheklaydi. Blokirovkani yechish uchun plastik hisob raqamiga yoki “davlat hamyoni”ga 310.000 so‘m miqdorida jarima to‘lashi zarurligiga ishontiradi. Aslida, ushbu holat raqamli qurilmani vaqtincha bloklab qo‘yilganiga ishontirish orqali amalga oshiriladi.

O‘zbekiston Respublikasi Oliy sudi Plenumining 2017 yil 11 oktabrdagi ***“Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”***gi 35-son qaroriga muvofiq “firibgarlikda yolg‘on ma‘lumotlarga jabrlanuvchini yanglishtirishga olib kelishi mumkin bo‘lgan har qanday holatlar, jumladan, yuridik fakt va voqealar, mulkning sifati, narxi, aybdorning shaxsi, uning vakolati, niyati (masalan, aybdor shaxs o‘zini mansabdor shaxs yoki huquqni muhofaza qiluvchi organ xodimi sifatida ko‘rsatishi) taalluqli bo‘lishi mumkin” – deyiladi<sup>12</sup>.

### **Jinoyat izlari**

Bank kartalaridan foydalanish bilan bog‘liq firibgarlik jinoyati natijasida qoldirilgan izlarni o‘rganish jinoyatni o‘z vaqtida aniqlash va tezkor ochish imkonini beradi. Jinoyat izlari kriminalistik tavsif elementlaridan biri bo‘lib, hosil bo‘lish mexanizmi jinoyatning moddiy va virtual olam bilan o‘zaro munosabati xarakteridan kelib chiqadi<sup>13</sup>.

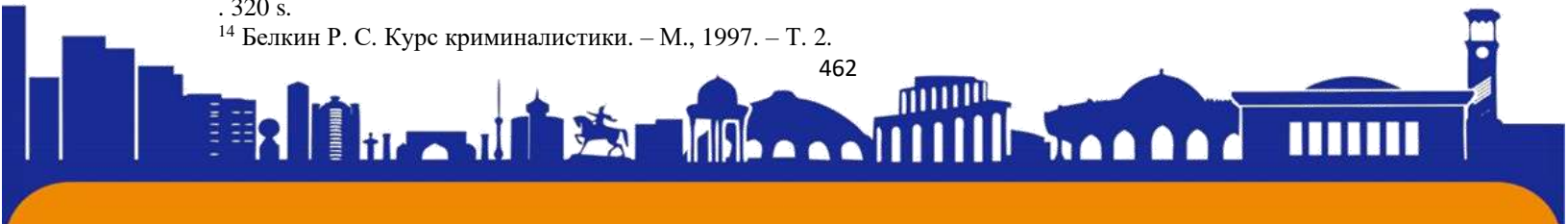
Taniqli kriminalist olim R.S. Belkin izlarni moddiy va ideal izlarga bo‘lishni taklif qilgan. Ideal izlar deganda u jinoyat sodir etgan shaxsning, guvoh yoki boshqa ishtirokchilarning xodirasida saqlangan izlar tushuniladi<sup>14</sup>. Raqamli texnologiyalarning rivojlanib borishi bilan nazariyada “virtual” yoki “raqamli” izlar tushunchalari ilmiy doira vakillari orasida keng muhokamalarga sabab bo‘lmoqda.

Kriminalistik adabiyotlarda “virtual” yoki “raqamli” izlar tushunchasi borasida turli xil qarashlar mavjud. Xususan, V.A.Agibalov, V.A.Mesheryakovlar virtual iz bu kompyuter tizimi orqali raqamli moddiy tashuvchida qayd qilingan real (fizik) jarayonni tasvirlovchi yoki ushbu jarayonning raqamli shakldagi rasmiy (matematik)

<sup>12</sup> Ўзбекистон Республикаси Олий суди Пленумининг 2017 йил 11 октябрдаги “Фирибгарликка оид ишлар бўйича суд амалиёти тўғрисида”ги 35-сон қарори 4-банднинг иккинчи хатбошиси.

<sup>13</sup> Meshcheryakov V.A. Prestupleniya v sfere kompyuternoy informatsii: pravovoy i kriminalisticheskiy analiz [Crimes in the sphere of computer information: legal and forensic analysis]. Voronezh, Voronezh State University, 2001 . 320 s.

<sup>14</sup> Белкин Р. С. Курс криминалистики. – М., 1997. – Т. 2.





modelidir, ya'ni jinoyat bilan bog'liq bo'lgan kompyuter tizimining boshqa harakatlari natijasi deyishadi<sup>15</sup>.

V. A. Mesheryakov izlarning uchinchi guruhi sifatida virtual izlarni kiritish kerakligini ta'kidlaydi. Uning fikricha, virtual izlar binar ko'rinishda namoyon bo'lib, faqatgina dasturiy vositalarni ishlatuvchi qurilmalar hamda axborotni o'ziga qabul qilishga yaroqli bo'lgan raqamli qurilmalarda qoladi<sup>16</sup>.

Internet orqali sodir etiladigan jinoyatlarda anonimlikni saqlash prinsiplial ahamiyatga ega. Shunga qaramay, ushbu jinoyatlarning deyarli barchasida texnik tavsifdagi izlar mavjud.

O.Y.Vedenskaya raqamli izlar ro'yxatiga IP-adreslar, ro'yxatdan o'tgan domen nomlari, foydalanuvchilarning akkaunt ma'lumotlari, log-fayllar, cookie fayllari, tashrif buyurilgan saytlar kesh fayl ma'lumotlari (vaqtinchalik fayllar) va brauzer tarixi, DNS-serverlar bilan bog'liq izlar, xosting-provayderlardagi izlar, reklama veb-sahifalari izlari, jabrlanuvchi raqamli qurilmasida saqlanib qolgan yozishmalar, qabul qilingan buyurtmalar izlari, mobil qurilma unikal raqami (IMEI), sim karta ma'lumotlari, bank karta hisob raqamlari, hisob raqamlardagi pul tushumi va chiqimi bilan bog'liq izlarni kiritgan<sup>17</sup>.

**Kesh-xotira** – inglizcha “cache memory” ya'ni, protsessor faoliyatini kutishdan xalos qiladigan tezlik bilan ishlaydigan buferli xotira qurilmasi bo'lib, juda katta tezlik bilan ishlaydigan protsessorlarning paydo bo'lishi, kesh-xotirani yaratish zaruratini keltirib chiqargan. Shu bilan birga, murakkab amaliy dasturlarning bajarilishi uchun katta xotira zarur edi. Shu sababli, operativ xotira bilan protsessor orasiga, kichkina sig'imli yuqori tezlikli kesh-xotira deb atalgan buferni o'rnatish amaliyoti boshlangan. Buning ustiga, uni protsessor ichiga o'rnatilgan va tashqi turlari mavjud<sup>18</sup>.

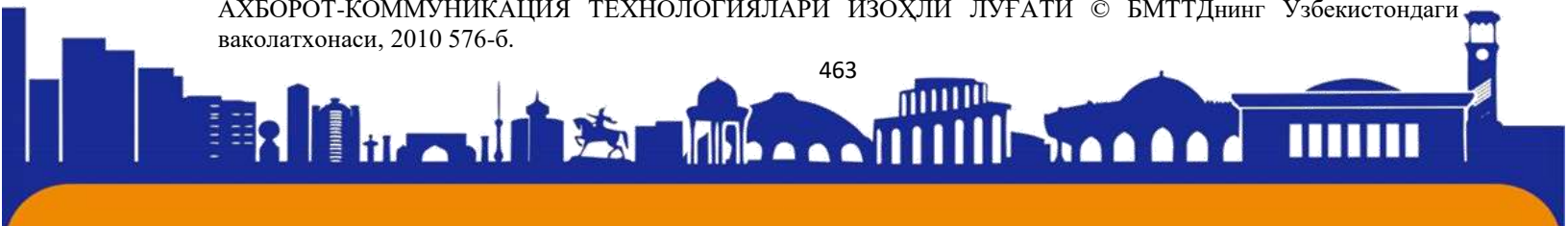
**DNS keshi** – bu inglizcha “domain name service” ya'ni, barcha so'nggi tashriflar va boshqa veb-sayt IP manzillariga kirishga urinishlar yozuvlarini o'z ichiga

<sup>15</sup> Агибалов В.А., Мещеряков В.А. Природа и сущность виртуальных следов, «Воронежские криминалистические чтения», Выпуск 12, Воронеж, 2010. С. 17-19.

<sup>16</sup> Meshcheryakov V.A. Prestupleniya v sfere kompyuternoy informatsii: osnovi teorii praktiki rassledovaniya. – Voronij, 2002.

<sup>17</sup> Юридическая наука и правоохранительная практика 4 (34) 2015 Введенская О.Ю. Особенности слеодообразования при совершении преступлений посредством сети интернет. С 213-214.

<sup>18</sup> Амиров Д.М., Атаджанов А.Ю., Атаджанов Д.Ю., Ибрагимов Д.А., Раҳимжонов З.Ё., Саидхўжаев С.С. АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ИЗОҲЛИ ЛУҒАТИ © БМТТДнинг Ўзбекистондаги ваколатхонаси, 2010 576-б.



olgan vaqtinchalik ma'lumotlar bazasidir. DNS keshi raqamli qurilma sahifaga yana tashrif buyurganingizda, ular tezroq ochilishi uchun qulaylik yaratadi.

**URL** – bu inglizcha “Uniform Resource Locator” ya’ni, resurs joyining universal ko‘rsatkichidir.

**Kyesh fayllar (vaqtinchalik fayllar)** – bu HTML - fayllar nusxasi, veb-saytga kirgan paytta yuklanadigan suratlar va boshqa kichik fayllar. Bu ma'lumotlar lokal diskda saqlanib, yana shu sahifaga qaytganda sahifani tezroq yuklanishiga yordam beradi.

**Brauzer tarixida** quydagi ma'lumotlar saqlanadi:

1. Tashrif buyurilgan sahifa va yuklangan ma'lumotlar (rasm, dasturlar, kino, musiqa va boshqalar);
2. Qidiruv buyurug‘lari va matnlari;
3. Veb saytdan avtorizatsiyadan utganlik haqida ma'lumotlar;
4. Kesh ma'lumotlar<sup>19</sup>.

**Sookie fayllari** – bu ushbu faylni yaratgan veb-sayt manzilini, o‘zgaruvchan qiymatlarini, ushbu sookie yaratilgan vaqtni o‘z ichiga oladi. Ushbu fayllar veb-server tashabbusi bilan foydalanuvchi kompyuterida saqlanadi va serverga foydalanuvchining individual sozlamalarini saqlash imkonini berish uchun mo‘ljallanadi.

Yuqorida keltirilgan izlar serverlarda, tarmoqda, jinoyat sodir etgan shaxs va jabrlanuvchilarning kompyuterlari yoxud boshqa texnik qurilmalarida saqlanib qolishi mumkin. Ushbu izlarni tiklashda ekspertlar “**EnCase**”, “**FTK**”, “**Pasco**” kabi dasturlardan foydalanishadi<sup>20</sup>. Ammo, tezkor qidiruv xodimlari tomonidan olib borilgan tezkor tadbirlarda va tergov harakatlarida har doim ham ko‘zlangan maqsadga erishilmaydi. Buning sababi, jinoyatchilar ko‘p hollarda jinoyat izlarini o‘chirib yuboruvchi dasturlardan, boshqa shaxslarning nomiga olingan abonent raqamlaridan, jinoyatga umuman aloqasi bo‘lmagan shaxslarning bank kartalaridan hisob raqamlaridan yoxud elektron hamyonlardan foydalanishadi. Shu orqali huquqni muhofaza qiluvchi organlarni chalg‘itishga urinishadi.

Jinoyatning issiq izidan borishda tergov va tezkor qidiruv xodimlari shaxsga doir ma'lumotlarni to‘plash maqsadida aloqa kompaniyalariga, bank yoki elektron to‘lov tizimlari operatorlariga so‘rov jo‘natishadi. Aloqa operatorlari shaxsni ro‘yxatdan

<sup>19</sup> И.А. Калмыков, В.С Пелешенко. Компьютерная криминалистика - Ставрополь: СКФУ, 2017, - 84 с.

<sup>20</sup> И.А. Калмыков, В.С Пелешенко. Компьютерная криминалистика - Ставрополь: СКФУ, 2017, - 84 с.



o'tgan sim kartalari, IMEI – raqamlari, kiruvchi va chiquvchi qo'ng'iroqlar sms xabarlarini haqidagi barcha ma'lumotlarni taqdim etishadi.

Shu bilan birga, jinoyatchini ushlashda bank tomonidan taqdim etilgan ma'lumotlar ham muhim ahamiyat kasb etadi. Ushbu ma'lumotlarga banklar tomonidan taqdim etiladigan shaxsga doir ma'lumotlar, pul ko'chirish bilan bog'liq moliyaviy operatsiyalar, onlayn bank ma'lumotlari, valyuta konvertatsiyasi va boshqa ma'lumotlar kiradi<sup>21</sup>.

Bank kartalari bilan bog'liq firibgarlik jinoyatlarida hodisa sodir etilgan joyni aniqlash masalasi boshqa jinoyatlarga qaraganda ancha mushkul hisoblanadi. Sababi, bu toifadagi jinoyatlarda jinoyatchi asosan boshqa davlatdan turib jinoyatni sodir etadi. Ko'p hollarda jinoyatchilar pullarni boshqa pul birligiga konvertatsiya qilib, bir davlat hududidan boshqa davlat hududiga o'tkazib yuborishadi va bu holat ishni yanada chigallashtirib, yurisdiksiya (ekstraditsiya) bilan bog'liq muammolarni keltirib chiqaradi.

#### **Shart-sharoitlar (vaqti, joyi va boshqa holatlar)**

Yuqoridagi jinoyat turi kriminalistik tavsifining elementi sifatida jinoyat sodir etish shart-sharoitlari hozirda uncha o'rganilmagan jabhalardan biridir. Bu haqda o'quv materiallari ham hali yetarlicha yozilmagan.

Ushbu jinoyatga qo'l urgan jinoyatchilar jinoyatni sodir etishda aniq bir vaqt yoinki joy tanlashmaydi. Bu turdagi jinoyatchilar kunning har qanday paytida, biror bir bino ofisida, o'z uyida, ko'chada yoki avtobus bekatida ham jinoyatni sodir etib ketaverishadi. Jinoyatchilar o'z manzilini yashirish maqsadida VPN yoki virtual mashinadan foydalanishadi.

**VPN** - virtual xususiy tarmoq ya'ni, (Virtual Private Network) bu umum foydalanishidagi ma'lumotlar uzatish tarmog'i (Internet) asosida tunnellash protokollari va trafikni shifrlash vositalaridan foydalangan holda qurilgan himoyalangan ma'lumotlarni uzatish tarmog'idir. Ma'lumotlarni uzatish muhiti sifatida mavjud bo'lgan kommunikatsiya infratuzilmasi, masalan Internet tarmog'idan foydalanuvchi tarmoq. Xavfsizlik masalalari uzatilayotgan ma'lumotlarni shifrlash va

---

<sup>21</sup> Lavrushkina A. A. Tipichnie sledstvennie deystviya v ramkax metodiki rassledovaniya moshennichestva s ispolzovaniem seti Internet i sredstv mobilnoy svyazi [Typical investigative actions within the methodology for investigating fraud using the Internet and mobile communications] Byulleten nauki i praktiki. 2018. T. 4. №4. S. 447-451. Rejim dostupa: <http://www.bulletennauki.com/lavrushkina-a> (data obrasheniya 15.04.2018).





beruxsat foydalanishning oldini olishning qator mexanizmlaridan foydalanish orqali ta'minlanadi<sup>22</sup>.

Jinoyat huquqida jinoyat sodir etilgan joy hodisa joyi hisoblanadi. Ammo, onlayn firibgarlikda esa, hodisa joyini aniqlash ancha mushkul jarayon hisoblanadi. Bu holat ayni damda jinoyatchilarning masofadan turib raqamli texnologiyalardan foydalangan holda, ba'zi dasturiy ta'minot, qurilmalarning va zararli dasturlar orqali jinoyat sodir etilgan joyni yashirishga urinishda ifodalanadi.

Ko'p hollarda jinoyatchilar pullarni boshqa pul birligiga konvertatsiya qilib, bir davlat hududidan boshqa davlat hududiga o'tkazib yuborishadi va bu holat ishni yanada chigallashtirib, yurisdiksiya (ekstraditsiya) bilan bog'liq muammolarni keltirib chiqaradi.

### **Jinoyatchi shaxsi**

Jinoyatchi shaxsini kriminalistik jixatdan o'rganish ijtimoiy-demografik, psixologik va biologik xususiyatlarni o'z ichiga oladi. Kriminalistikada jinoyatchi shaxsi uning individual xususiyatlari va fazilatlarini bilish orqali belgilanadi. Ushbu sohadagi jinoyatni sodir etganlar orasida yuqori malakali mutaxassislar, turli darajadagi ta'lim va ijtimoiy mavqega ega bo'lgan shaxslar yoxud havaskor jinoyatchilar bo'lishi mumkin. Shuningdek, "xakerlar"ni ya'ni kiberjinoyatchilarni ham bir nechta turga ajratish mumkin.

### **Karder**

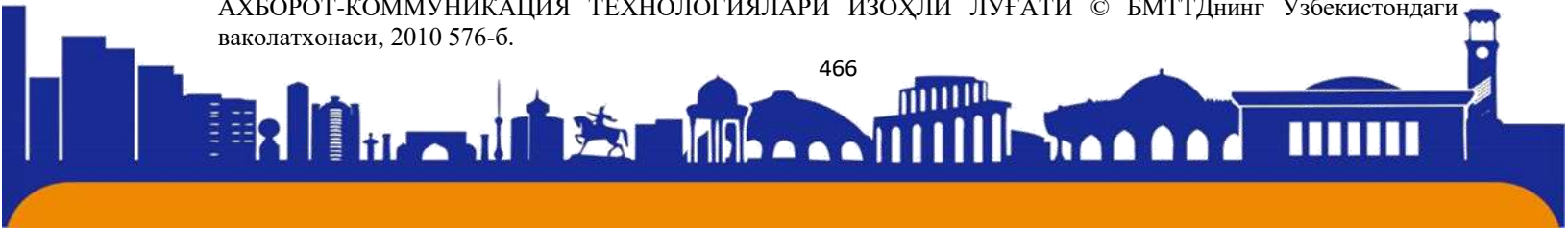
Karderlar bu bank plastik kartalari (karta raqami, to'liq nomi, amal qilish muddati, xavfsizlik kodi) ma'lumotlarini to'plash, o'g'irlash bilan shug'ullanadigan shaxs yoki bir guruh shaxslardir. Ular asosan xizmat ko'rsatish sohasida ya'ni ko'pincha ofitsiant yoki do'kon sotuvchisi bank xodimi sifatida faoliyat yuritib, mijozlarning plastik kartalaridagi ma'lumotlarini ularga sezdirmasdan o'g'rilashadi va ushbu ma'lumotlardan firibgarlik sodir etishda foydalanishadi.

### **Fisher**

Fisherlar ya'ni, ijtimoiy tarmoqlardagi sahifalarni buzib kiruvchi jinoyanchilar. Ular ijtimoiy tarmoqdagi moliyaviy daromadi ancha yuqori bo'lgan shaxslarning

---

<sup>22</sup> Амиров Д.М., Атаджанов А.Ю., Атаджанов Д.Ю., Ибрагимов Д.А., Раҳимжонов З.Ё., Саидхўжаев С.С. АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ИЗОҲЛИ ЛУҒАТИ © БМТТДнинг Ўзбекистондаги ваколатхонаси, 2010 576-б.





ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF(2023)-3,778 Volume-1, Issue-12

sahifalariga o'zlarini "do'stlar qatoriga" qo'shdirib ushbu shaxslar haqidagi ma'lumotlarni o'rganishadi va ulardan firibgarlik sodir etishda foydalanishadi.

Ushbu turdagi jinoyatlar ko'pincha bank xodimlari, sobiq xodimlar, IT-sohasida muayyan tajriba, bilim va ko'nikmaga ega shaxslar tomonidan sodir etiladi. Internet firibgarligi bilan shug'ullanuvchi shaxslarni olim I.M.Rusakov ikkita katta guruhga ajratadi:

birinchi guruhda, o'z mansab vakolati chegarasidan chiqib jinoyat sodir etadigan xodimlar, ya'ni texnik personal, xizmatchilar, xavfsizlikni ta'minlovchi xodimlar, boshqaruv xodimlari, tashkiliy masalalar bilan shug'ullanuvchi xodimlar. Bundan tashqari, operatorlar, dasturchilar, injenerlar va kompyuter axborotlariga ruxsatsiz kirishi mumkin bo'lgan boshqa shaxslar.

ikkinchi guruhga, kompyuter tizimi xavfsizligi uchun javobgar shaxslar, professional mutaxassislar va yuqori salohiyatga ega dasturchilarni kiritgan. Bu turdagi firibgarlar odatda jinoyatga oldindan puxta tayyorgarlik ko'rishi, uzgacha fikrlashi, kompyuter atamalariga bog'liq lahjada gapirishi bilan boshqa turdagi jinoyatchilardan farq qiladi<sup>23</sup>.

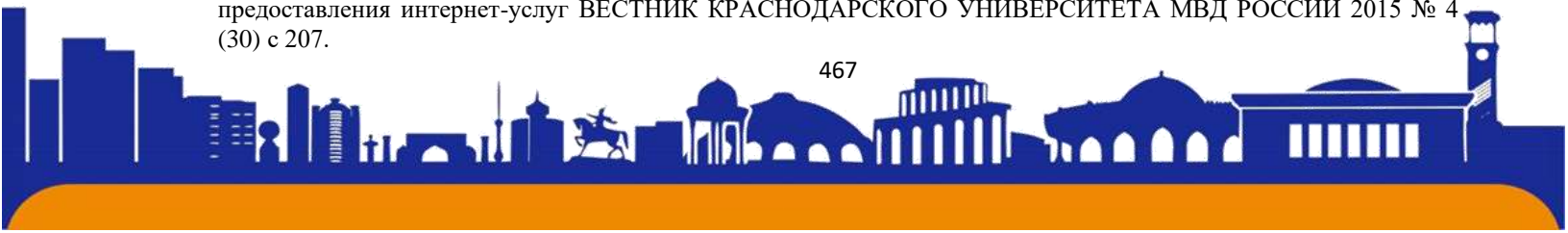
## XULOSA

Xulosa qilib aytganda, raqamli texnologiyalarning shiddat bilan rivojlanib borishi yangi munosabatlar vujudga kelishiga sabab bo'lmoqda. Biroq, ushbu munosabatlarni o'z vaqtida nazorat qilish va tartibga solish muayyan kriminalistik va huquqiy tadqiqotlarni olib borishni taqozo etmoqda. Aks holda, inson, jamiyat va davlat manfaatlarini turli iqtisodiy, siyosiy, huquqiy va ma'naviy tahdidlar ostida qolishi ayni haqiqatdir. Amaldagi qonunchilikda onlayn firibgarlik, o'g'rilik va tovlamachilik jinoyatlarini kvalifikatsiya qilish bo'yicha huquqiy bo'shliqlarning mavjudligi huquqni qo'llash sohasida muayyan uslubiy qiyinchiliklarni ham yuzaga keltirmoqda.

Shunga ko'ra, amaldagi qonunchilikni takomillashtirish hamda huquqiy tartibga solishning samarali mexanizmlarini joriy etish bo'yicha quyidagilar taklif etiladi:

1. O'zbekiston Respublikasining Jinoyat kodeksida "elektron to'lov tizimlari bilan bog'liq firibgarlik jinoyati", "bank hisob raqami yoki elektron to'lov tizimlari

<sup>23</sup> Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг ВЕСТНИК КРАСНОДАРСКОГО УНИВЕРСИТЕТА МВД РОССИИ 2015 № 4 (30) с 207.





ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF(2023)-3,778 Volume-1, Issue-12

bilan bog‘liq o‘g‘rilik jinoyatlari” kabi alohida moddalarni belgilash (ushbu moddalar Rossiya Federatsiyasi Jinoyat qonunchiligida mavjud);

2. Ushbu jinoyatlar yuzasidan alohida Oliy sud Plenumi qarorlarini va amaliyot xodimlariga mo‘ljallangan ilmiy, amaliy o‘quv qo‘llanmalarni ishlab chiqish;

3. O‘zbekiston Respublikasining 2022-2026 yillarga mo‘ljallangan Harakatlar strategiyasida kiberjinoyatlarni tergov qilish uslubiyotini takomillashtirish bo‘yicha alohida vazifalar belgilash;

4. O‘zbekiston Respublikasining “To‘lov va to‘lov tizimlari to‘g‘risida”gi qonunida to‘lov tashkilotlari (operatori) tomonidan amalga oshirilayotgan onlayn moliyaviy xizmatlar xavfsizligini ta‘minlash uchun to‘lov xizmatlaridan foydalanuvchilarni autentifikatsiya qilishning samarali mexanizmlarini joriy qilish;

5. Kadrlar masalasiga alohida e‘tibor qaratish, xorijiy mutaxassislarni jalb qilgan holda tergov va sud tizimi xodimlarini kiberjinoyatlarni tergov qilish bilan bog‘liq bilim va ko‘nikmalarini shakllantirish maqsadida, o‘quv kurslarini tashkil etish va ularni malakasini oshirish.

Ushbu islohotlar o‘z navbatida qonunni to‘g‘ri va o‘z o‘rnida qo‘llashga, yuqorida keltirilgan jinoyatlarni oldini olishga va jinoyatchilikka qarshi murosasiz kurashishga xizmat qiladi.

## REFERENCES

1. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет. Дисс. на соис. уч. степ. канд. юрид. наук. – Пятигорск, 2010. – С. 24.

2. Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества. Владимир, 2002. – 211 с.

3. Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. № 4. С. 19-21.

4. Лопашенко Н.А. Посягательства на собственность: монография. – М.: Норма, Инфра-М, 2012. – С. 8.

5. Жиноятларни тергов қилишнинг криминалистик методикаси: Ўқув қўлланма / Р.Р. Шакуров, Ш.Т. Джуманов, Н. Тоштемиров, Д.Р. Тураева, О.Д. Алланазаров. – Т: Ўзбекистон Республикаси ИИВ академияси, 2013. – 5 б.





6. Криминалистика. Дарслик. Муаллифлар жамоаси. Абдумажидов Ф.А. ва б.қ. – Т.: Адолат, 2003. Т. 2. – 74 б.
7. Бахин В.П. Криминалистическая характеристика преступлений как элемент расследования // Вестник криминалистики. – Москва, 2006. – Вып. 1. – С. 140.
8. Кудрявцев Д.С. Особенности криминалистической характеристики убийств, замаскированных под безвестное исчезновение человека // Актуальные проблемы современной криминалистики и судебной экспертизы: материалы междунар. науч.-практ. конф., посвящ. 35-летию со дня образования кафедры криминалистики Акад. МВД Респ. Беларусь (Минск, 3 июня 2011 г.). – Минск: Акад. МВД, 2011. – С.160.
9. Белкин Р.С. Криминалистика: Учебник для вузов. – М., 2001. – С. 126.
10. Шаззо С.К. Способи совершения мошенничества в отношении граждан [Метходс оф коммиттинг фразд агаинст ситизенс]. Вестник Адигейского государственного университета. Серия 1: Юриспруденция. 2008. № 2. С.
11. Табак И.С. Мошенничество с банковскими картами / И.С. Табак // Современные инновации. – 2018. – № 4 (26). – № 1 (19). – С. 37-40.
12. Kozodaeva O. N., Obidenova A. S. Spособи soversheniya moshennichestva sispol`zovaniem bankovskix kart [Ways to commit fraud using bank cards]. Uchenie zapiski Tambovskogo otdeleniya RoSMU. S. 52.
13. Ўзбекистон Республикаси Олий суди Пленумининг 2017 йил 11 октябрдаги “Фирибгарликка оид ишлар бўйича суд амалиёти тўғрисида”ги 35-сон қарори 4-банднинг иккинчи хатбошиси.
14. Белкин Р. С. Курс криминалистики. – М., 1997. – Т. 2.
15. Агибалов В.А., Мещеряков В.А. Природа и сущность виртуальных следов, «Воронежские криминалистические чтения», Выпуск 12, Воронеж, 2010. С. 17-19.
16. Meshcheryakov V.A. Prestupleniya v sfere kompyuternoy informatsii: osnovi teorii praktiki rassledovaniya. – Voronij, 2002.
17. Юридическая наука и правоохранительная практика 4 (34) 2015 Введенская О.Ю. Особенности слеодообразования при совершении преступлений посредством сети интернет. С 213-214.

