

UDC: 343.72(045)(575.1)

BANK KARTALARIDAN FOYDALANISH BILAN BOG'LIQ FIRIBGARLIK JINOYATLARINING KRIMINALISTIK TAHLILI

Hamidov Baxtiyor Hamidovich,

Toshkent davlat yuridik universiteti
Kriminalistika va sud ekspertizasi kafedrası
katta o'qituvchisi
ORCID: 0000-0002-8097-5056
e-mail: Bahtiyor1984bsj@mail.ru

Nosirov Amirxon Bahodir o'g'li,

Toshkent davlat yuridik universiteti 4-kurs talabasi
ORCID: 0000-0002-8097-5056
e-mail: A.nosirov.1111tsul@gmail.com

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, mualliflik xulosalari shakllantirilgan. Qonun chiqaruvchi va uni qo'llovchi subyektlar 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.

КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ МОШЕННИЧЕСКИХ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

Хамидов Бахтиёр Хамидович,

старший преподаватель кафедры
Криминалистика и судебная экспертиза
Ташкентского государственного юридического университета

Носиров Амирхон Баходир угли,

студент 4-курса
Ташкентского государственного юридического университета

Аннотация. В статье дан криминалистический анализ мошеннических преступлений, связанных с использованием банковских карт. Он содержит элементы криминалистического описания мошенничества, связанного с использованием банковских карт, – предмет преступления, способы совершения преступления, следы преступления, личные данные преступника, обстоятельства преступления. При этом критически рассмотрен процесс работы с цифровыми следами при расследовании мошенничества с банковскими картами, проблемы, возникающие в национальном законодательстве и правоприменительной практике. Разработаны научно обоснованные способы и критерии их устранения. Кроме того, обсуждено сходство интернет-мошенничества как одного из видов интернет-преступности с мошенничеством с банковскими картами. Статья подготовлена на основе научно-практических исследований и мнений ученых-теоретиков и юристов-практиков в сфере работы, связанной с цифровыми следами. В статье анализируются проблемы в данной области с систематической, правовой, научной и практической точек зрения, из которых сформированы авторские выводы. Также разработаны научно обоснованные предложения и рекомендации для законодателей и правоохранительных органов.

Ключевые слова: банковские карты, мошенничество, связанное с банковскими картами, следы преступления, способ преступления, личность преступника, электронные платежные системы.

FORENSIC ANALYSIS OF FRAUDULENT CRIMES WITH THE USE OF BANK CARDS

Khamidov Bakhtiyor Khamidovich,

Senior lecturer of Tashkent State University of Law

Amirkhon Nosirov Bahodirovich

Student of Tashkent State University of Law

Abstract. This article describes the general concept and forensic analysis of the crime of fraud associated with the use of bank cards. It contains elements of forensic description of the crime of fraud associated with the use of bank cards, the subject of the crime, methods of committing a crime, traces of the crime, personal information of the offender, and the circumstances of crime. At the same time, the process of working with digital footprints in the investigation of bank card fraud, the problems that arise in national legislation and law enforcement practices, have all been critically examined. Scientifically based ways and criteria for their elimination have been developed. In addition, the similarities of Internet fraud, a type of Internet crime, with bank card fraud were discussed. The article is based on scientific and practical research in the field of working with digital traces, the views of theoretical scientists and practitioners, as well as technical research. The article analyzes the problems in the field from a systematic, legal, scientific, and practical point of view, which from the author's conclusions are formed. Evidence-based proposals and recommendations for legislators and law enforcement agencies have been developed.

Keywords: bank cards, bank card fraud, traces of the crime, criminal method, criminal identity, electronic payment systems.

Kirish

Bozor iqtisodiyoti va raqamli texnologiyalarning takomillashib borishi insoniyat hayotining turli jabhalari, xususan, bank munosabatlari, sanoat, xizmat ko'rsatish va boshqa sohalar rivojiga samarali ta'sir ko'rsatmoqda.

Mamlakatdagi raqamlashtirish jarayonlari hamda onlayn xizmatlar bozoridagi talab va taklifning ortib borishi bank kartalarining qulay to'lov tizimiga aylanishiga olib keldi. Natijada naqd to'lovlarsiz moliyaviy hisob-kitoblarni amalga oshirish kundalik ehtiyojlar-

ni qondirishning ajralmas qismiga aylanib ulgurdi.

Bugungi kunda tijorat banklari tomonidan “Uzkard” hamda “Humo” to’lov tizimlarining milliy valyutadagi bank kartalari muomalaga chiqarilib, ularning infratuzilmasi kengayib bormoqda. O’zbekiston Respublikasi Vazirlar Mahkamasining 2004-yil 24-sentabrdagi “Plastik kartalar orqali hisob-kitob tizimini yanada rivojlantirish chora-tadbirlari to’g’risida”gi 445-sonli qaroriga asosan, yagona umumrespublika protsessing markazi tashkil etilib, “Uzkard” to’lov tizimi faoliyat yurita boshladi. 2020-yil 11-aprelda Yagona umumrespublika protsessing markazi MCHJ-ga “Uzkard” to’lov tizimi operatori litsenziyasi Markaziy bank tomonidan taqdim etildi. O’zbekiston Respublikasi Prezidentining 2018-yil 19-sentabrdagi “Milliy to’lov tizimini rivojlantirish chora-tadbirlari to’g’risida”gi 3945-sonli qaroriga asosan, Milliy banklararo protsessing markazi tashkil etilib, 2019-yilning II choragidan boshlab “Humo” to’lov tizimi ishga tushirildi. Milliy banklararo protsessing markazi MCHJga 2020-yil 11-aprelda “Humo” to’lov tizimi operatori litsenziyasi Markaziy bank tomonidan berildi. Mamlakatimizda bank kartalari infratuzilmasi 2020-yil 1-yanvar holatiga 20 547 ming dona bank kartalari, 392 361 ta to’lov terminallari hamda 9 203 ta bankomat va infokiosklardan tashkil topgan. 2019-yil davomida ikkita milliy chakana (“Humo” hamda “Uzkard”) to’lov tizimlarining Visa, Master Kard, China Union Pay hamda Mir xalqaro to’lov tizimlari bilan integratsiyasi samarali amalga oshirildi [1].

Onlayn xizmatlar bozorining o’sib borishi kiberjinoyatlarning turli shakl va turlari kirib kelishiga ham sabab bo’lmoqda. Xususan, onlayn firibgarlik jinoyati ana shunday shiddat bilan o’sib borayotgan jinoyatlardan biri sanaladi.

Firibgarlar tomonidan bank kartalaridan pul yechib olishning yangidan-yangi usul va vositalari qo’llanilishi jinoyat mexanizmlari

murakkablashuviga olib kelmoqda. Statistik ma’lumotlarga tayanib, shuni aytish mumkin, ki, 2019-yilda sodir etilgan firibgarlik jinoyati 6 321 tani tashkil etgan bo’lsa, 2020-yil davomida esa 10 496 tani tashkil qilgan [2]. Demak, firibgarlik jinoyati 2020-yilda 42% ga o’sganligini ko’rishimiz mumkin.

Onlayn firibgarlik jinoyati fosh etilishi juda qiyin bo’lgan jinoyatlardan biri bo’lib, puxta rejalashtirilganligi, o’ta murakkabligi hamda transmilliy xususiyatga egaligi bilan boshqa turdagi jinoyatlardan farq qiladi. Onlayn firibgarlik tushunchasi ba’zi kriminalistik adabiyotlarda kiberfiribgarlik, ba’zilarida esa kompyuter firibgarligi deb keltiriladi.

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 [3, 211-b.]. M.A. Yefremova esa kiberfiribgarlik va kompyuter firibgarligini bir xil tushuncha, ya’ni sinonimlar deb hisoblaydi [4, 19-21-b.].

Qonunchiligimizda onlayn firibgarlik, kiberfiribgarlik, bank kartalaridan foydalanish bilan bog’liq firibgarlik jinoyati tushunchalari 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 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.*

Odatda, pul, qimmatbaho buyumlar, texnika va boshqa ashyolar firibgarlik jinoyatining predmeti sanaladi. Ammo bank kartalaridan foydalanish bilan bog'liq firibgarlik jinoyatining bevosita predmeti bu o'zganing mulki, ya'ni o'zgalarning bank karta hisobraqamlarida saqlanayotgan pulidir. Biroq to'g'ridan to'g'ri bank kartasining o'zi jinoyat predmeti bo'la olmaydi, chunki jinoyatchining motiv-maqsadi faqatgina karta hisobraqamlarida 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 elementidir. Chunki u jinoyatga tayyorgarlik ko'rish, amalga oshirish va jinoyatni yashirish bo'yicha jinoyatchilarning harakatlarini yagona maqsadda bir-lashtiradi.

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

Material va metodlar

Maqola raqamli izlar bilan ishlash sohasida amalga oshirilgan ilmiy-amaliy tadqiqotlar, nazariyotchi olimlar hamda amaliyotchi xodimlar fikr-mulohazalari asosida tayyorlangan. Maqolada sohada yuzaga kelayotgan muammolar tizimli, huquqiy, ilmiy-amaliy jihatdan tahlil etilgan, mualliflik xulosalari shakllantirilgan.

Tadqiqot natijalari

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 [5, 5-b.].

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

“Fishing” bilan shug'ullanuvchi jinoiy gu-ruhlar jabrlanuvchidan shaxsiy ma'lumotlari-ni kiritishni so'rab, turli shaklda xabarnoma jo'natadi. Jabrlanuvchi bank xizmatlaridan foydalanish uchun bankning rasmiy veb-say-tiga kirayotganliklariga ishonadi. Biroq firib-garlar tuzog'iga laqqa tushadilar. Xususan, soxta saytga ism-sharifi, karta rekvizitlari, pin kodi kiritish orqali o'zlari bilmagan holda “fishing”chilar qarmog'iga ilinadi [6, 49–52]. Soxta saytlar yaratish – bu zamonaviy fishing uslublaridan biridir. Bunday fishing saytlari-ni maxsus bilim va ko'nikmalarsiz aniqlash juda mushkul. Bundan tashqari, fishingchilar xuddi shu usulni aloqa vositalari, ya'ni to'g'ri-dan to'g'ri telefon orqali bog'lanib ham sodir etishlari mumkin.

Xuddi shunday holatlar mamlakatimiz-da ham kuzatilib, o'zini “Click xodimi” deb tanishtirgan shaxslar tizimdagi ayrim kam-chiliklarni tuzatish hamda to'lov bilan bog'liq buzilishlarning oldini olish niqobi-da jabrlanuvchiga sms jo'natib, undan sms raqamini aytishini so'rashyapti. SMS raqami aytilishi bilan pul mablag'lari turli plastik kartalar yoki telefon raqamlarga tranzaksi-ya qilinadi. Shundan so'ng Click orqali Qiwi hamyonga o'tkaziladi va jinoiy yo'l bilan un-dirilgan pul mablag'lari (so'm) xorijiy va-lyutaga konvertatsiya qilinadi.

Meros firibgarligi

Jabrlanuvchi nomiga chet eldagi qarindoshidan katta miqdordagi meros qoldiril-gani haqidagi xabar go'yoki uning advokati niqobida beriladi. Shundan so'ng pasport

hamda plastik karta raqamlariga doir maxfiy 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 maxfiy ma'lumotlar aldov yo'li bilan olinadi.

Fishing tanlovlar

Ijtimoiy tarmoqlarda soxta tanlovlar tashkil qilish. Bu holatda yutuq sifatida avtotransport vositasi yoki oxirgi rusumli telefon apparati qo'yiladi. E'tiborli jihati shundaki, tashkilotchilar deyarli barcha ishtirokchilarni "Siz lotoreyada g'olib chiqdingiz yoki sovg'alar soni cheklangan, aksiyada ishtirok eting, sovg'ani qo'lga kiriting" kabi yutuq bilan tabriklab yoxud tanlovda ishtirok etishi uchun qiziqtirib xabar jo'natadi. Odatda, fishing tanlovi ishtirokchilari tanlovda bir necha marotaba ishtirok etganidan so'ng ushbu jarayon firibgarlik ekanligiga tushunib yetadi.

Internet-tilanchilik – soxta xayriya jamg'armalari

Internet sahifalari hamda ijtimoiy tarmoqlarga turli xil kasallikka chalingan yoxud og'ir ahvoldagi shaxslarning fotosuratlarini joylashtirib, ularning nomidan moddiy yordam so'rash. Firibgarlar ko'proq insoniylik, rahm-shafqat va ishonuvchanlik his-tuyg'ularini uyg'otuvchi psixologik ta'sir etish usullariga e'tibor qaratadi. Odatda, nomi e'lon qilinayotgan shaxslar ular uchun pul mablag'lari jamg'arilayotgani haqida hech qanday ma'lumotga ega bo'lmaydi. 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

Ba'zi firibgarlar qalbaki, sifatsiz tovar yoki mahsulotlar savdosi bilan shug'ullanib, xaridorlarni chuv tushirsa, boshqalari mahsulot uchun oldindan qisman yoki to'liq to'lov qilishni talab qiladi [7, 52-b.]. 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'lari 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 tegishli fotosuratlardan foydalanib, ularning nomidan jabrlanuvchilar bilan yozishmalar olib boradi va ishonchiga kiradi. Vaqt 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 meykerlik va boshqa shakldagi onlayn xizmatlari ko'rsitishdir. Ushbu usulning 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, quyidagi vaziyat bunga yaqqol misol bo'la oladi. Jinoyatchilar internet tarmog'idagi pornografik materiallar, shafqatsizlikni targ'ib qiluvchi saytlarda o'zlarini huquqni muhofaza qiluvchi organlar yoxud IIV Kiberxavfsizlikka qarshi kurash

bo'limi tomonidan foydalanuvchi ma'muriy javobgarlikka tortilgani va ma'lum bir pul miqdorini belgilangan hisobraqamga 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 hisobraqami yoki davlat hamyoniga 310 000 so'm miqdorida jarima to'lashingiz zarur" [8].

Odatda, bunday noqulay vaziyatdan tezroq chiqish hamda sharmandalik va javobgarlikdan qutulish maqsadida talab qilingan pul summasi tegishli hisobraqamga o'tkaziladi. Biroq, afsuski, IIV Kiberjinoyatlarga qarshi kurash bo'limi hech kimga bunday xabar yubormaydi...

Ushbu holat o'zida firibgarlik alomatlarini ham mujassamlashtirgan. Sababi, birinchidan, jinoyatchi o'zini huquqni muhofaza qiluvchi organ xodimi deb tanishtirib, jabrlanuvchini aldaydi. Ikkinchidan, jinoyatchi jabrlanuvchining internet tarmog'idan foydalanish huquqini muayyan vaqt oralig'ida cheklaydi. Blokirovkani yechish uchun plastik hisobraqami yoki "davlat hamyoni"ga 310 000 so'm miqdorida jarima to'lashi zarurligiga ishonitiradi. Aslida, ushbu holat raqamli qurilmaning vaqtincha bloklab qo'yilganiga ishonitirish 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.

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 [9, 64-b.].

Raqamli texnologiyalarning rivojlanib borishi bilan nazariyada "virtual" yoki "raqamli" izlar tushunchalari ilmiy doira vakillari orasida keng muhokamalarga sabab bo'lmoqda [10, 74–76-b.].

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) modelidir, ya'ni jinoyat bilan bog'liq bo'lgan kompyuter tizimining boshqa harakatlari natijasi deyishadi [11, 17–19-b.]. Bundan tashqari, huquqshunos olimlardan biri I. Astanov ham raqamli izlar va raqamli dalillar sohasida yuqoridagi olimlar kabi bir qancha tadqiqotlar olib borgan [12, 265–266-b.].

Internet orqali sodir etiladigan jinoyatlarda anonimlikni saqlash prinsipial ahamiyatga ega. Shunga qaramay, ushbu jinoyatlarining deyarli barchasida texnik tavsifdagi izlar mavjud. O.Y. Vvedenskaya raqamli izlar ro'yxatiga IP-adreslar, ro'yxatdan o'tgan domen nomlari, foydalanuvchilarning akkaunt ma'lumotlari, log-fayllar, 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, bank karta hisobraqamlari, hisobraqamlardagi pul tushumi va chiqimi bilan bog'liq izlarni kiritgan [13, 213-214-b.].

Yuqorida keltirilgan izlar server, tarmoq, jinoyat sodir etgan shaxs va jabrlanuvchilarning kompyuterlari yoxud boshqa texnik qurilmalarida saqlanib qolishi mumkin. Ammo tezkor qidiruv xodimlari tomonidan olib borilgan tezkor tadbirlarda va tergov harakatlari har doim ham ko'zlangan maqsadga erishilmaydi. Buning sababi, jinoyatchilar ko'p hollarda boshqa shaxslarning nomiga olingan abonent raqamlaridan yoki jinoyatga umuman aloqasi bo'lmagan shaxslarning bank kartalari, hisobraqamlaridan 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 shaxs ro'yxatdan o'tgan sim kartalari, IMEI raqamlari, kiruvchi va chiquvchi qo'ng'iroqlar sms xabarlari haqidagi barcha ma'lumotlarni taqdim etadi. Shu bilan birga, jinoyatchini ushlashda bank tomonidan taqdim etilgan ma'lumotlar ham muhim ahamiyat kasb etadi [14, 447-b.]. 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.

Bank kartalari bilan bog'liq firibgarlik jinoyatlarida hodisa sodir etilgan joyni aniqlash masalasi boshqa jinoyatlarga qaraganda ancha mushkul. Sababi bu toifadagi jinoyatlarda jinoyatchi, asosan, boshqa davlatdan turib jinoyat sodir etadi [15, 448-b.]. Ko'p hollarda jinoyatchilar pullarni boshqa pul birligiga konvertatsiya qilib, bir davlat hududidan boshqa davlat hududiga o'tkazib

yuboradi va bu holat ishni yanada chigallashtirib, yurisdiksiya (ekstraditsiya) bilan bog'liq muammolarni keltirib chiqaradi.

Ushbu jinoyatga qo'l urgan jinoyatchilar jinoyatni sodir etishda aniq vaqt va joy tanlamaydi. Bu turdagi jinoyatchilar biror-bir bino ofisida, o'z uyida, ko'chada yoki avtobus bekatida ham jinoyat sodir etib ketaveradi. Jinoyatchilar o'z manzilini yashirish maqsadida VPN yoki virtual mashinadan foydalani-shadi.

Jinoyatchi shaxsi

Bu turdagi jinoyatlar bank xodimlari, sobiq xodimlar, bank va IT-sohasida muayyan tajriba, bilim va ko'nikmaga ega shaxslar tomonidan sodir etiladi. Internet firibgarligi bilan shug'ullanuvchi shaxslarni olim I.M. Rusa-kov 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 guruhda, kompyuter tizimi xavfsizligi uchun javobgar shaxslar, professional mutaxassislar va yuqori salohiyatga ega dasturchilar. Bu turdagi firibgarlar, odatda, jinoyatga oldindan puxta tayyorgarlik ko'rishi, o'zgacha fikrlashi, kompyuter atamalariga bog'liq lahdada gapirishi bilan boshqa turdagi jinoyatchilardan farq qiladi [16, 207-b.].

Xulosalar

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 tadqiqotlar olib borishni taqozo etmoqda. Aks holda, inson, jamiyat va davlat manfaatlari turli iqtisodiy, siyosiy, huquqiy va ma'naviy tahdidlar ostida qolishi hech gap emas. Amalda-

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

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

3. 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 foydalanuvchini autentifikatsiya qilishning samarali mexanizmlarini joriy qilish maqsadga muvofiq.

Ushbu islohotlar, o'z navbatida, qonunni to'g'ri va o'z o'rnida qo'llash, yuqorida keltirilgan jinoyatlarning oldini olish va jinoyatchilikka qarshi murosasiz kurashishga xizmat qiladi.

REFERENCES

1. O'zbekiston Respublikasida to'lov tizimining rivojlanish bosqichlari [Stages of development of the payment system in the Republic of Uzbekistan]. Available at: <https://cbu.uz/oz/payment-systems/history/>.
2. Huquqbuzarlik. Jinoyat va adolat statistikasi [Offense. Crime and Justice Statistics]. Available at: <https://stat.uz/uz/rasmiy-statistika/crime-and-justice-2/>.
3. Zikov D.A. Viktimologicheskie aspekti preduprezhdeniya kompyuternogo moshennichestva [Victimological aspects of computer fraud prevention]. Vladimir, 2002, 211 p.
4. Yefremova M.A. Moshennichestvo s ispolzovaniem elektronnoy informatsii [Fraud using electronic information]. *Informatsionnoe parvo – Information law*, 2013, no. 4, pp. 19-21.
5. Shazzo S.K. Sposobi soversheniya moshennichestva v otnoshenii grajdan [Methods of committing fraud against citizens]. *Vestnik Adigeyskogo gosudarstvennogo universiteta – Bulletin of the Adyghe State University*, Series 1 – Jurisprudence, 2008, no. 2, p. 5.
6. Izotov D.S., Bikova N.N. Vidi moshennichestva s bankovskimi kartami [See bank card fraud]. *Vestnik NGIEI – Bulletin of NGIEI*, 2015, no. 3, pp. 49-52.
7. Kozodaeva O.N., Obidenova A.S. Sposobi soversheniya moshennichestva s ispolzovaniem bankovskix kart [Ways to commit fraud using bank cards]. *Uchenie zapiski Tambovskogo otdeleniya RoSMU – Scientific notes of the Tambov branch of Rostu*, p. 52.
8. Bud' ostorozhen! Moshenniki v internete [Be careful! Internet scammers]. Available at: <https://iiv.uz/news/ogoh-boling-internet-tarmogida-firibgarlar/>.
9. Filippov A.G. Kriminalistika [Criminalistics]. Moscow, Spark Publ., 2000, 520 p.
10. 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 p.
11. Agibalov V.A., Meshcheryakov V.A. Priroda i sushnost virtualnix sledov [The nature and essence of virtual footprints]. *Voronezhskie kriminalisticheskie chteniya – Voronezh forensic readings*, 2010, iss. 12, pp. 17-19.

12. Astanov I.I., Hamidov B. Obshcheteoreticheskie voprosi, svyazannie s elektronnyimi ili sifrovimi dokazatel'stvami: problema i reshenie [General theoretical issues related to electronic or digital evidence: problem and solution]. *Obshchestvo i innovatsii – Society and innovation*, 2021, no. 2, 7/S, pp. 259-278. DOI: 10.47689/2181-1415-vol2-iss7/S-pp259-278/.

13. Vvedenskaya O.Y. Osobennosti sledoobrazovaniya pri sovershenii prestupleniy posredstvom seti internet [Features of trace formation when committing crimes via the Internet]. *Legal science and law enforcement practice*, pp. 213-214.

14. 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 – Bulletin of Science and Practice*, 2018, vol. 4, no. 4, pp. 447-451. Available at: <http://www.bulletennauki.com/lavrushkina-a/> (accessed 15.04.2018).

15. Kriminalisticheskaya xarakteristika lichnosti prestupnika, sovershivshego moshennichestvo v sfere predostavleniya internet-uslug [Forensic characterization of the identity of the criminal who committed fraud in the provision of Internet services]. *Vestnik Krasnodarskogo Universiteta MVD Rossii – Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia*, 2015, no. 4, p. 207.

YURISPRUDENSIYA

HUQUQIY ILMIY-AMALIY JURNALI

2 / 2022

BOSH MUHARRIR:

Nodirbek Salayev

Ilmiy ishlar va innovatsiyalar bo'yicha prorektor

BOSH MUHARRIR O'RINBOSARI:

Ikrom Ergashev

Ilmiy boshqarma boshlig'i

Mas'ul muharrir: D. Xudoynazarov

Muharrirlar: Sh. Jahonov, K. Abduvaliyeva,
F. Muhammadiyeva, Y. Yarmolik

Texnik muharrirlar: U. Sapayev, D. Rajapov

Tahririyat manzili:

100047. Toshkent shahar, Sayilgoh ko'chasi, 35.

Tel.: (0371) 233-66-36, 233-41-09.

Faks: (0371) 233-37-48.

Web-sayt: www.tsul.uz

E-mail: lawjournal@tsul.uz

E-mail: tn.tdyu@mail.ru

Jurnal 05.05.2022-yilda tipografiyaga topshirildi.

Qog'oz bichimi: A4. Shartli 20,88 b.t. Adadi: 100.

Buyurtma: № 14.

TDYU tipografiyasida chop etildi.