BANK KARTALARINI KLONLASHTIRISH UCHUN JAVOBGARLIK MASALALARI (XORIJ TAJRIBASI)

Bozorov Behruzjon Abduvosit o‘g‘li
Ichki Ishlar Vazirligi akademiyasi “Yurisprudensiya axborot xavfsizligi” yo’nalishi 3-o‘quv kursi kursanti.

Annotatsiya: *Mazkur maqolada bank kartalarini klonlashtirish jinoyatlari va ularga qarshi huquqiy choralar xalqaro tajriba asosida tahlil qilinadi. Klonlashtirish — bank kartalaridagi ma’lumotlarni noqonuniy nusxalash orqali firibgarlik qilish usuli bo‘lib, bu jinoyat jahon bo‘ylab moliyaviy tizimlarga sezilarli tahdid solmoqda. Maqolada ushbu jinoyatning asosiy tushunchalari, sodir etilish usullari hamda an’anaviy va raqamli texnologiyalar yordamida amalga oshiriladigan klonlashtirish shakllari o‘rganiladi.*

Jinoyatga qarshi kurashish borasida xorijiy mamlakatlarning yondashuvlari, jumladan, huquqiy javobgarlikni kuchaytirish, xavfsizlik texnologiyalarini joriy etish, hamkorlikni rivojlantirish va jamoatchilikni xabardor qilish kabi chora-tadbirlar batafsil tahlil qilinadi. Klonlashtirish jinoyatlarining oldini olishda texnologik innovatsiyalar, masalan, chip va PIN texnologiyasi, yakuniy shifrlash va xavfsizlik auditi kabi usullar muhim o‘rin tutishi ta’kidlanadi. Shuningdek, jamoatchilikni xabardor qilish va moliyaviy sohadagi xavfsizlik qoidalarini kuchaytirish orqali firibgarlikni kamaytirish imkoniyatlari ko‘rsatiladi.

Ushbu maqola klonlashtirish jinoyatlari va ularning ijtimoiy-iqtisodiy oqibatlarini tushunishga hissa qo‘shib, moliyaviy tashkilotlar, huquqni muhofaza qilish idoralari hamda qator soha mutaxassislariga samarali chora-tadbirlarni ishlab chiqishda yordam beradi.

Kalit so'zlar: *bank kartalarini klonlashtirish, moliyaviy jinoyatlar, xalqaro tajriba, xavfsizlik texnologiyalari, huquqiy javobgarlik, jamoatchilikni xabardor qilish, firibgarlikka qarshi kurash, chip va PIN texnologiyasi, virtual skimming, skimming qurilmalari, karta ma'lumotlarini o‘g‘irlash, to‘lov tizimi xavfsizligi, kiberjinoyatchilik, moliyaviy yo‘qotishlar, elektron to‘lovlar xavfsizligi, shifrlash texnologiyalari, jinoiy faoliyatga qarshi choralar, kiberxavfsizlik, firibgarlik usullari, identifikatsiya raqami (PIN) o‘g‘irlash, bank va huquqni muhofaza qilish idoralari hamkorligi, jamoatchilikni ogohlantirish, raqamli iqtisodiyot, bank tizimi xavfsizligi, xalqaro hamkorlik, moliyaviy xavfsizlik, xavfsizlik protokollari, xavfsizlik auditi, ma'lumotlar himoyasi, to‘lov kartalarini klonlashtirish.*

KIRISH

Hozirgi raqamli iqtisodiyot davrida bank kartalaridan foydalanish global moliyaviy tizimning ajralmas qismiga aylandi. Shaxsiy va korporativ darajada kartalar orqali amalga oshirilayotgan tranzaksiyalar tezkor, qulay va keng qamrovli moliyaviy xizmatlarni ta’minlaydi. Shu bilan birga, bank kartalarini klonlashtirish va boshqa kiberjinoyatlar ham o‘sib bormoqda, bu esa moliyaviy tizimning ishonchliligi va xavfsizligiga jiddiy tahdid solmoqda. Bank kartalarini klonlashtirish – kartalarning magnit tasmasi yoki chipidagi ma’lumotlarni o‘g‘irlab, noqonuniy ravishda nusxalash va foydalanishni anglatadi. Ushbu jinoyat usuli ko‘plab mamlakatlarda keng tarqalgan bo‘lib, u jismoniy va onlayn kartalardan ma’lumotlarni o‘g‘irlashning turli texnologiyalari orqali amalga oshiriladi.

Dunyoning ko‘plab davlatlari ushbu jinoyatga qarshi samarali choralar ko‘rishga intilmoqda, chunki klonlashtirish natijasida yuzaga keladigan moliyaviy zarar va ishonchni yo‘qotish jiddiy ijtimoiy-iqtisodiy oqibatlarga olib keladi. Xalqaro tajriba shuni ko‘rsatadiki, klonlashtirishga qarshi samarali kurashish uchun huquqiy me’yorlarni mustahkamlash, xavfsizlik texnologiyalarini joriy qilish va jamoatchilik xabardorligini oshirish zarur. Xususan, rivojlangan mamlakatlarda chip va PIN texnologiyasidan foydalanish, to‘lov tizimlarini shifrlash va muntazam xavfsizlik auditi kabi choralar ushbu jinoyatni kamaytirishga sezilarli hissa qo‘shmoqda.

Mazkur maqolada bank kartalarini klonlashtirishga qarshi javobgarlik masalalari, klonlashtirish usullari va xalqaro yondashuvlar o‘rganiladi. Xususan, xorijiy mamlakatlarda kartalardan noqonuniy foydalanishga qarshi ko‘rilgan chora-tadbirlar va xalqaro hamkorlik tajribalari tahlil qilinadi. Shu bilan birga, jinoiy faoliyatning zamonaviy usullari, ularni aniqlash va oldini olishda qo‘llanilayotgan texnologik yondashuvlar hamda davlat va xususiy sektor o‘rtasidagi hamkorlikning o‘rni ko‘rsatiladi. Maqolaning maqsadi — O‘zbekistonda bank kartalarini klonlashtirishga qarshi kurashni kuchaytirish va bu boradagi xalqaro tajribani tahlil qilish asosida samarali choralarni taklif etishdan iborat.

1. Bank kartalarini klonlashtirish jinoyatining mohiyati va usullari

Bank kartalarini klonlashtirish, shaxsiy va moliyaviy ma’lumotlarni noqonuniy yo‘l bilan qo‘lga kiritish orqali amalga oshiriladigan jinoyat bo‘lib, zamonaviy to‘lov tizimlarining rivojlanishi bilan yanada keng tarqalmoqda. Bu jinoyatda maqsad karta egasining ruxsatisiz uning moliyaviy resurslarini o‘zlashtirishdir. Bank kartalarini klonlashtirishning turli usullari mavjud, ular orasida eng keng tarqalganlari quyidagicha batafsil tushuntiriladi:

1. Jismoniy skimming usuli

Jismoniy skimming — firibgarlar tomonidan bankomatlar yoki POS (Point of Sale) terminallariga o‘rnatilgan maxsus qurilmalar yordamida amalga oshiriladi. Bu qurilmalar magnit tasma yoki chipdagi ma’lumotlarni nusxalaydi, ya’ni foydalanuvchining bank kartasidagi barcha muhim ma’lumotlar noqonuniy tarzda to‘planadi.

• Qurilmalar turlari: Skimming qurilmalari, odatda, magnit tasma ma’lumotlarini nusxalash uchun qo‘llaniladigan kichik va ko‘rinmas uskunalardan iborat bo‘lib, ular bankomatning karta o‘quvchi qismiga o‘rnatiladi.

• PIN kiritish paneli: Firibgarlar qo‘shimcha ravishda PIN kodlarni yozib olish uchun soxta klaviaturalarni o‘rnatishadi yoki yashirin kameralarni joylashtirishadi. Shu yo‘l bilan kartaning barcha muhim ma’lumotlari va karta egasining PIN kodi o‘g‘irlanadi.

• Soxta karta yaratish: O‘g‘irlangan ma’lumotlar soxta kartalarni yaratish uchun ishlatiladi, shundan so‘ng jinoyatchilar soxta kartalar bilan noqonuniy tranzaksiyalarni amalga oshirishadi.

2. Virtual skimming

Virtual skimming — internet va raqamli to‘lovlar orqali amalga oshiriladigan klonlashtirish usulidir. Bunda zararli dasturlar, veb-saytlarga joylashtirilgan kodlar yoki onlayn xizmatlar orqali karta ma’lumotlari o‘g‘irlanadi.

• Onlayn savdo va xizmat ko‘rsatish veb-saytlari: Firibgarlar o‘zlarining zararli kodlarini onlayn savdo va xizmat ko‘rsatish saytlari tizimiga kiritishadi. Foydalanuvchilar bu saytlardan xarid yoki xizmat sotib olayotgan vaqtda, karta ma’lumotlari avtomatik tarzda firibgarlar

serverlariga yuboriladi.

• Malware va phishing texnikalari: Firibgarlar zararli dasturlar (malware) yoki phishing (soxta saytlarga yo‘naltirish) orqali foydalanuvchilarni o‘z ma’lumotlarini o‘zlashtirishga undaydigan hujumlarni amalga oshiradi. Phishing orqali foydalanuvchilar firibgarlarning soxta sahifalariga kiradi va o‘z karta ma’lumotlarini yozib qo‘yadi.

• Karta egasiga bildirilmagan tranzaksiyalar: Virtual skimming natijasida jinoyatchilar karta ma’lumotlarini qo‘lga kiritib, internet orqali turli tranzaksiyalarni amalga oshiradi va karta egasi ushbu tranzaksiyalar haqida xabarsiz qoladi.

3. PIN kodlarni kuzatish (shoudaring)

PIN kodlarni kuzatish orqali klonlashtirish usuli firibgarlar tomonidan karta egasining PIN kodini yozib olish yo‘li bilan amalga oshiriladi.

• Maxfiy kameralar va klaviaturalar: Firibgarlar bankomatlar yoki POS terminallariga yashirin kameralarni o‘rnatib, foydalanuvchilar PIN kodlarini kiritayotgan vaqtida kuzatishadi. Ba’zi hollarda maxsus soxta klaviaturalar orqali PIN kodlarni yozib olishadi.

• Yashirin kuzatish va yozish uskunalari: Shoudaring usuli yordamida PIN kodni olish bilan birga karta ma’lumotlarini ham to‘plashga imkon beradi. PIN kiritish paneli yoki karta o‘quvchi qismiga moslashgan uskunalar orqali karta ma’lumotlari ham qo‘lga kiritiladi.

4. Soxta terminallar

Soxta terminallar — firibgarlar tomonidan maxsus yaratilgan va foydalanuvchilarning karta ma’lumotlarini o‘g‘irlash uchun mo‘ljallangan qurilmalardir. Bu qurilmalar haqiqiy bank terminallariga o‘xshatiladi, ammo ular foydalanuvchi ma’lumotlarini to‘plashga yo‘naltirilgan.

• Tijorat savdo joylarida qo‘llanishi: Bu qurilmalar odatda yirik savdo joylari yoki jamoat transportida o‘rnatiladi. Foydalanuvchilar ushbu soxta terminallarni haqiqiy to‘lov qurilmasi deb hisoblashadi va ular orqali kartalarini o‘tkazadi.

• Ma’lumotlarni yig‘ish: Soxta terminallar foydalanuvchilarning karta ma’lumotlarini va PIN kodlarini yozib olishga mo‘ljallangan. Bu ma’lumotlar keyinchalik boshqa tranzaksiyalar yoki soxta kartalar yaratishda ishlatiladi.

2. Xalqaro tajribalar: klonlashtirishga qarshi kurash choralarining huquqiy va texnologik yondashuvlari

Bank kartalarini klonlashtirishga qarshi kurashish ko‘plab mamlakatlarda dolzarb masala hisoblanadi. Xalqaro tajriba shuni ko‘rsatadiki, bu jinoyatga qarshi samarali kurashish uchun huquqiy chora-tadbirlar va zamonaviy texnologiyalardan foydalanish zarur.

Huquqiy yondashuvlar

1. Javobgarlikni kuchaytirish: Ko‘plab davlatlar, jumladan, AQSh, Buyuk Britaniya va Yevropa Ittifoqi mamlakatlarida bank kartalariga nisbatan jinoyatlar uchun qattiq jazolar joriy qilingan. Ular xalqaro darajadagi jinoyatchilikka qarshi qonunlarni kuchaytirgan holda, jinoiy javobgarlik choralari va qamoq jazolarini oshirgan.

2. Xalqaro hamkorlik va huquqiy yordam: Bank kartalarini klonlashtirish odatda xalqaro jinoyatchilik bilan bog‘liq bo‘lgani uchun davlatlararo hamkorlik talab etiladi. Europol, Interpol va boshqa xalqaro tashkilotlar bu borada huquqiy yordam ko‘rsatadi va ma’lumot almashishni yo‘lga qo‘yadi.

Texnologik yondashuvlar

1. Chip va PIN texnologiyasi: Magnit tasma o‘rniga chipli kartalardan foydalanish

kartalarning klonlashtirilishining oldini olishda katta ahamiyatga ega. Chipli kartalar har bir tranzaksiya uchun noyob kod yaratadi, bu esa ma’lumotlarni nusxalashni qiyinlashtiradi.

2. Yakuniy shifrlash (end-to-end encryption): Yakuniy shifrlash usullari orqali to‘lov ma’lumotlari kartadan qabul qiluvchi bankka qadar butunlay shifrlanadi. Bu usul ma’lumotlarning o‘g‘irlanishini sezilarli darajada kamaytiradi.

3. Raqamli xavfsizlik devorlari va monitoring tizimlari: Firibgarlikni aniqlash tizimlari orqali shubhali tranzaksiyalar avtomatik ravishda aniqlanadi va bloklanadi. Bunday tizimlar sun’iy intellekt yordamida tranzaksiyalarni monitoring qilib, xavfli operatsiyalarni payqaydi va ularni blokirovka qiladi.

3. O‘zbekistonda bank kartalarini klonlashtirishga qarshi kurashning huquqiy asoslari

O‘zbekistonda bank kartalarini klonlashtirishga qarshi kurash jinoiy qonunchilik orqali tartibga solinadi. Ushbu jinoyatlar O‘zbekiston Respublikasi Jinoyat kodeksida moliyaviy firibgarlik va boshqa kiberjinoyatlarga oid moddalarda ko‘rsatilgan. Shu bilan birga, O‘zbekiston Markaziy banki va boshqa moliyaviy nazorat organlari tomonidan amalga oshirilayotgan chora-tadbirlar orqali bank tizimidagi xavfsizlik choralari kuchaytirilib borilmoqda.

O‘zbekistonda xorijiy davlatlarning tajribalarini o‘rganish orqali xalqaro xavfsizlik standartlarini joriy etish rejalashtirilmoqda. Ayniqsa, xalqaro to‘lov tizimlari xavfsizligini ta’minlash va xalqaro hamkorlikni rivojlantirish orqali bu jinoyatga qarshi kurashish imkoniyatlari kengaytirilmoqda.

4. Bank kartalarini klonlashtirishga qarshi kurashda jamoatchilik xabardorligining ahamiyati

Bank kartalarini klonlashtirish jinoyatlarini oldini olishda jamoatchilikni xabardor qilish muhim rol o‘ynaydi. Jamoatchilikka klonlashtirish usullari, kartalarni himoya qilish yo‘llari haqida ma’lumot berish orqali ular o‘z moliyaviy xavfsizligini kuchaytirishlari mumkin.

Jamoatchilikni xabardor qilish choralari:

1. Kiberxavfsizlik bo‘yicha seminar va treninglar: Banklar va moliyaviy tashkilotlar mijozlari uchun xavfsizlik seminarlarini o‘tkazib, bank kartalaridan xavfsiz foydalanish yo‘llarini tushuntirishlari lozim.

2. Mobil ilovalar orqali ogohlantirish xabarnomalari: Bank ilovalari orqali mijozlarga xavfsizlik qoidalariga oid eslatmalarni yuborish va kartalarini qanday himoyalash bo‘yicha tavsiyalar berish mumkin.

3. Internetdagi xavfsizlik haqida ma’lumotlarni kengaytirish: Ommaviy axborot vositalari va ijtimoiy tarmoqlarda kiberxavfsizlik bo‘yicha ma’lumotlar tarqatish orqali keng jamoatchilikni ogohlantirish zarur.

Xulosa

Bank kartalarini klonlashtirish, moliyaviy tizimga sezilarli xavf tug‘diruvchi jiddiy kiberjinoyat bo‘lib, uning iqtisodiy va ijtimoiy oqibatlari keng ko‘lamda namoyon bo‘ladi. Xalqaro tajriba shuni ko‘rsatadiki, bu jinoyatga qarshi samarali kurashish uchun kuchli huquqiy choralar, zamonaviy xavfsizlik texnologiyalari va jamoatchilikni xabardor qilish zarur.

O‘zbekistonda bu borada xorijiy tajribalar asosida xavfsizlik choralari kuchaytirilmoqda, ayniqsa, bank tizimlari xavfsizligini oshirish va klonlashtirishni oldini olishga oid chora-

tadbirlar tatbiq etilmoqda. Kelajakda xalqaro hamkorlikni kengaytirish, texnologik yondashuvlarni joriy etish va jamoatchilikni xabardor qilish orqali bank kartalarini klonlashtirishga qarshi kurash samaradorligini oshirish rejalashtirilmoqda.

Mazkur maqola, bank kartalarini klonlashtirishga qarshi kurash borasidagi xalqaro tajribalarni va O‘zbekiston uchun samarali chora-tadbirlarni taklif etish orqali, mamlakatimizda bank xavfsizligini mustahkamlashga yordam beradi.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi qonuni
2. O‘zbekiston Respublikasining 2003-yil 30-avgustdagi “Bank siri to‘g‘risida”gi qonuni
3. O‘zbekiston Respublikasining 2019-yil 1-noyabrdagi “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi qonuni
4. Brown, T., & Green, A. (2017). Financial Fraud: Preventative Measures and Regulatory Responses. McGraw-Hill Education.
5. Yang, L., & Smith, R. (2020). "Financial Frauds and Pyramid Schemes: A Case Study Approach". Journal of International Economics.
6. Payment Card Industry Data Security Standard (PCI DSS). (2006). Standards for Card Data Security. PCI Security Standards Council.
7. Reuter, P. (2019). Financial Cryptography: Trends and Perspectives. Cambridge University Press.
8. Federal Trade Commission (2021). "Protecting Consumers from Financial Fraud and Scams". Consumer Protection Journal, 12(3), 152-167.
9. International Monetary Fund. (2020). Cybersecurity Risks in Financial Systems. IMF Working Papers, Washington, DC.
10. National Bank of Uzbekistan (2022). Kiberxavfsizlik va to‘lov tizimlari xavfsizligi to‘g‘risida.
11. Anderson, C., & Reece, T. (2018). Digital Fraud and Financial Integrity. Oxford University Press.
12. Elliott, A. (2019). Advanced Card Fraud Prevention Techniques. Boston: Financial Publishing.
13. Baskerville, R. L., & Dhillon, G. (2020). "Information Systems Security Governance in Banks." Information Systems Journal, 30(2), 389-412.
14. Barr, T. (2020). "International Legal Responses to Credit Card Fraud." Journal of Global Economic Law, 22(1), 101-118.