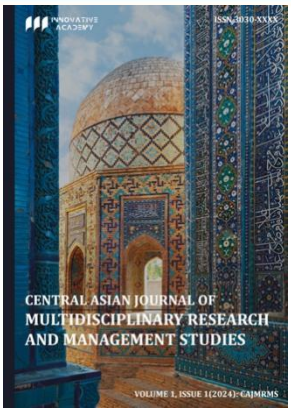

FUQAROLAR PLASTIK KARTALARI KIBERXAVFSIZLIGINI TA'MINLASH TIZIMINI TAKOMILLASHTIRISH

XO'JAXONOVA SITORA BAXTIYOR QIZI
TOSHKENT DAVLAT IQTISODIYOT UNIVERSITETI

https://doi.org/10.5281/zenodo.18918669

ARTICLE INFO

Received: 1st March 2026
Accepted: 5th March 2026
Published: 9th March 2026

KEYWORDS

Plastik karta, kiberxavfsizlik, naqd pulsiz hisob-kitob, ijtimoiy muhandislik, autentifikatsiya, uch bosqichli xavfsizlik, biometrik himoya, tranzaksiyalar monitoringi, sun'iy intellekt, moliyaviy xavfsizlik.

ABSTRACT

Mazkur maqolada fuqarolarning plastik kartalari bilan bog'liq kiberxavfsizlik muammolari chuqur tahlil qilinadi hamda raqamli iqtisodiyot sharoitida moliyaviy operatsiyalar xavfsizligini ta'minlash masalalari yoritiladi. So'nggi yillarda naqd pulsiz hisob-kitob tizimining kengayishi, onlayn to'lovlar hajmining ortishi va mobil bank xizmatlarining ommalashuvi plastik kartalar orqali amalga oshiriladigan operatsiyalar sonini keskin oshirdi. Bu esa o'z navbatida soxta internet sahifalari orqali ma'lumotlarni qo'lga kiritish, bankomat qurilmalari yordamida karta ma'lumotlarini yashirin nusxalash, zararli dasturlar orqali ma'lumot o'g'irlash hamda ijtimoiy muhandislik kabi kiberjinoyat turlarining ko'payishiga olib kelmoqda. Maqolada plastik kartalar xavfsizligiga tahdid soluvchi asosiy omillar, ularning kelib chiqish sabablari va iqtisodiy oqibatlari ilmiy asosda o'rganiladi. Shuningdek, bank tizimida qo'llanilayotgan mavjud himoya mexanizmlari – bir martalik parollar, uch bosqichli xavfsizlik texnologiyasi, biometrik autentifikatsiya, tranzaksiyalar monitoringi tizimlari – samaradorligi tahlil qilinadi. Maqolada kiberxavfsizlikni ta'minlash tizimini takomillashtirish bo'yicha amaliy taklif va tavsiyalar berilgan. Jumladan, ko'p bosqichli autentifikatsiya tizimini keng joriy etish, sun'iy intellekt asosida shubhali operatsiyalarni aniqlash mexanizmlarini rivojlantirish, real vaqt rejimida xavflarni monitoring qilish, bank va davlat organlari o'rtasida axborot almashinuvini kuchaytirish hamda fuqarolarning kiberxavfsizlik bo'yicha moliyaviy savodxonligini oshirish zarurligi asoslab beriladi.

KIRISH

Bugungi kunda O'zbekiston bank tizimi jadal raqamli transformatsiya jarayonidan o'tmoqda, bu esa fuqarolarning plastik kartalar orqali to'lovlar qilish amaliyotini sezilarli darajada oshirdi. So'nggi yillarda mamlakatda naqd pulsiz hisob-kitoblar ulushi muntazam ravishda ortib bormoqda, bunga to'lov kartalari, mobil ilovalar va internet bank

xizmatlarining jadal rivojlanishi sabab bo‘lmoqda. Milliy statistik ma’lumotlarga ko‘ra, plastik kartalar orqali amalga oshiriladigan operatsiyalar soni yillar davomida barqaror o‘sib, naqd pulsiz to‘lovlar umumiy hajmi sezilarli darajada oshgan. Masalan, Markaziy bank ma’lumotlariga ko‘ra, 2024 yilda banklararo to‘lovlar hajmi minglab trillion so‘mlarga yetdi va kontaktli hamda kontaktlarsiz texnologiyalar, shu jumladan “Tap-to-Phone”, Humo Pay va QR-kod orqali to‘lovlar faol joriy etildi. Bu raqamli to‘lovlar xizmatlarining qulayligi va ommaviyligi oshishiga yordam berdi.

Raqamli to‘lovlar xizmatlarining kengayishi bank tizimining samaradorligini oshirish bilan birga, fuqarolarga qulaylik yaratmoqda, biroq shu bilan birga yangi xavf va tahdidlarni ham yuzaga keltirmoqda. Jumladan, plastik kartalar orqali amalga oshiriladigan moliyaviy operatsiyalar sonining ko‘payishi axborot texnologiyalari asosidagi tizimlardagi zaif tomonlarni ham ko‘proq ko‘rsatmoqda. Bu holat nafaqat moliyaviy institutlar uchun, balki butun jamiyat uchun kiberxavfsizlik muammolarini yanada dolzarb masalaga aylantirmoqda.

Bank tizimidagi raqamli xizmatlarning keng qo‘llanilishi natijasida to‘lov tizimlarida axborot oqimlari va ma’lumotlar bazalari hajmi keskin ko‘paydi. Shu ma’noda plastik kartalar bilan bog‘liq operatsiyalarni amalga oshirish jarayonida yuzaga keladigan tahdidlar tizimli tarzda o‘rganilishi lozim. Axborot tizimlarida yuzaga keladigan xatoliklar yoki tizimli zaifliklar nafaqat shaxsiy ma’lumotlarni oshkor qilishi, balki moliyaviy yo‘qotishlarga ham olib kelishi mumkin.

Shu sababli mamlakatimizda banklar va moliyaviy boshqaruv organlar — ya’ni pul-kredit siyosatini yurituvchi Markaziy bank hamda boshqa moliyaviy institutlar — raqamli infratuzilmani mustahkamlashga, axborot xavfsizligi talablarini takomillashtirishga alohida e’tibor qaratmoqda. Ushbu e’tibor nafaqat texnik vositalarni joriy etishdan iborat emas, balki fuqarolarning moliyaviy savodxonligini oshirish, kiberxavfsizlik bo‘yicha targ‘ibot ishlari olib borish, xavf boshqaruvi tizimlarini integratsiya qilish kabi kompleks yondashuvlarni ham o‘z ichiga oladi.

Bu sharoitda plastik kartalar xavfsizligi masalalarini tizimli, ilmiy asosda o‘rganish va ularni bartaraf etish yo‘llarini aniqlash bugungi kunda nafaqat amaliy ahamiyatga, balki dolzarb bo‘lgan mavzuga aylanmoqda.

PLASTIK KARTALAR XAVFSIZLIGIGA TAHDIDLAR

Bugungi kunda O‘zbekiston bank tizimida plastik kartalar orqali amalga oshiriladigan moliyaviy operatsiyalar soni sezilarli darajada ortib bormoqda. Shu bois ushbu operatsiyalar xavfsizligini ta’minlash masalasi tobora dolzarb ahamiyat kasb etmoqda. Operatsiyalar hajmining oshishi bilan bir qatorda, ularga tahdid soluvchi xavf-xatarlar ham murakkablashib, yangi ko‘rinishlarda namoyon bo‘lmoqda.

Raqamli texnologiyalar va internet xizmatlarining jadal rivojlanishi fuqarolarga katta qulayliklar yaratdi: masofadan turib to‘lovlarni amalga oshirish, onlayn xaridlar, mobil ilovalar orqali bank xizmatlaridan foydalanish kundalik hayotning ajralmas qismiga aylandi. Biroq ushbu qulayliklar bilan birga plastik kartalar xavfsizligiga tahdid soluvchi yangi xatarlar — kiberfiribgarlik, fishing (phishing), zararli dasturlar orqali ma’lumotlarni o‘g‘irlash, ijtimoiy muhandislik usullari kabi jinoyat turlari ham kengaymoqda.

Statistik ma’lumotlarga ko‘ra, 2024-yilda mamlakatda jami 58,8 mingta kiberjinoyat holati qayd etilgan bo‘lib, ularning taxminan 97,7 foizi fuqarolarning plastik kartalari orqali pul o‘g‘irlash va turli firibgarlik sxemalari bilan bog‘liq. Ushbu raqamlar bank kartalari atrofida yuzaga kelayotgan muammolarning qanchalik jiddiy ekanini yaqqol ko‘rsatadi.

Shu munosabat bilan bank tizimida axborot xavfsizligini mustahkamlash, zamonaviy himoya mexanizmlarini joriy etish, mijozlarning moliyaviy savodxonligini oshirish hamda kiberxavfsizlik bo‘yicha profilaktik choralarni kuchaytirish muhim vazifaga aylanmoqda. Faqat kompleks yondashuv orqaligina plastik kartalar bilan bog‘liq moliyaviy operatsiyalar xavfsizligini ta’minlash va fuqarolarning mablag‘larini ishonchli himoya qilish mumkin.

O‘zbekiston bank tizimida plastik kartalar bilan bog‘liq eng ko‘p uchraydigan tahdidlarni quyidagicha guruhlab ko‘rsatish mumkin:

1. Ijtimoiy muhandislik
2. Soxta saytlar va havolalar orqali aldash
3. Telefon orqali firibgarlik va SMS orqali aldash
4. Zararli dasturlar
5. Bankomat qurilmasi orqali ma’lumot ko‘chirish
6. SIM-kartani noqonuniy almashtirish
7. Onlayn savdo orqali firibgarlik
8. Ochiq internet tarmoqlari orqali hujum
9. Ma’lumotlar bazasining sizib chiqishi
10. Ichki tahdidlar

1. Ijtimoiy muhandislik— bu firibgarlar tomonidan inson omilidan foydalanish orqali maxfiy ma’lumotlarni qo‘lga kiritish usulidir. Bunda jinoyatchilar texnik vositalardan ko‘ra ko‘proq psixologik ta’sir, ishonch uyg‘otish, qo‘rqitish yoki shoshiltirish kabi usullardan foydalanadi. Ularning asosiy maqsadi — fuqaroning bank kartasi rekvizitlari, parollari yoki tasdiqlash kodlarini olish orqali hisobidagi mablag‘ni o‘zlashtirishdir.

Ko‘pincha firibgarlar o‘zini bank xodimi sifatida tanishtirib qo‘ng‘iroq qiladi va “hisobingizda shubhali operatsiya aniqlandi”, “kartangiz bloklandi” yoki “kredit rasmiylashtirilmoqda” kabi yolg‘on ma’lumotlar bilan mijozni vahimaga soladi. Ayrim hollarda ular huquqni muhofaza qiluvchi organ vakili yoki texnik xizmat mutaxassisi sifatida ham chiqish qiladi.

Shuningdek, SMS yoki messenjerlar orqali aldov xabarlari yuborish ham keng tarqalgan. Masalan, “sizga pul o‘tkazildi”, “sovrin yutdingiz” yoki “kartangiz bloklanadi” kabi xabarlar orqali fuqaro zararli havolaga o‘tishga yoki shaxsiy ma’lumotlarini kiritishga undaladi.

Eng xavfli jihatlardan biri — tasdiqlash kodini so‘rab olishdir. Firibgar suhbat davomida yoki xabar orqali bankdan kelgan bir martalik kodni aytishni talab qiladi. Aslida esa bu kod pul o‘tkazmasini tasdiqlash uchun kerak bo‘ladi. Agar fuqaro ushbu kodni aytsa, jinoyatchi uning nomidan moliyaviy operatsiyani amalga oshirishi mumkin.

Xavfi:

- Bank hisobidagi mablag‘larning tezkor ravishda yechib olinishi
- Kredit rasmiylashtirib qo‘yilishi
- Shaxsiy ma’lumotlarning uchinchi shaxslarga tarqalishi

Oldini olish choralari:

- Bank xodimlari hech qachon tasdiqlash kodi yoki to‘liq karta ma’lumotlarini so‘ramasligini yodda tutish
- Noma’lum raqamlardan kelgan qo‘ng‘iroqlarga ishonmaslik
- Shoshilinch qaror qabul qilmaslik va suhbatni darhol to‘xtatish
- Shubhali holatlarda bankning rasmiy aloqa markaziga mustaqil ravishda qo‘ng‘iroq qilish
- Kartaga bog‘langan mobil ilovada bildirishnomalarni doimiy nazorat qilish

Ijtimoiy muhandislik bugungi kunda plastik kartalar bilan bog‘liq jinoyatlarning eng keng tarqalgan turi hisoblanadi, chunki u insonning ehtiyotsizligi va ishonuvchanligiga tayanadi. Shu sababli moliyaviy savodxonlik va hushyorlik eng muhim himoya vositasi sanaladi.

2. Soxta saytlar va havolalar orqali aldash- bu foydalanuvchini qalbaki internet sahifasiga yo‘naltirish va u yerda kiritilgan shaxsiy hamda moliyaviy ma’lumotlarni qo‘lga kiritishga qaratilgan firibgarlik usulidir. Ushbu usulda jinoyatchilar bank yoki to‘lov tashkilotining rasmiy saytiga juda o‘xshash veb-sahifalar yaratadi. Sahifa dizayni, logotipi va

manzil ko‘rinishi asl nusxaga o‘xshatiladi, natijada oddiy foydalanuvchi farqni sezmasligi mumkin.

Firibgarlar elektron pochta, SMS yoki Telegram orqali yolg‘on havolalar yuboradi. Xabarlarda odatda “hisobingiz bloklandi”, “xavfsizlikni tasdiqlang”, “to‘lovni qabul qiling” kabi shoshilinch mazmundagi ogohlantirishlar bo‘ladi. Foydalanuvchi havolaga kirib, foydalanuvchi nomi, parol, karta raqami yoki tasdiqlash kodini kiritganda, ushbu ma’lumotlar bevosita jinoyatchilar qo‘liga o‘tadi. Ba’zi hollarda soxta sayt orqali zararli dastur ham yuklab olinishi mumkin, bu esa qurilmadagi boshqa ma’lumotlarning ham o‘g‘irlanishiga sabab bo‘ladi.

Xavfi:

- Foydalanuvchi nomi va parol qo‘lga kiritilishi
- Karta rekvizitlari va tasdiqlash kodlari o‘g‘irlanishi
- Hisobdan noqonuniy pul o‘tkazmalari amalga oshirilishi
- Shaxsiy ma’lumotlarning tarqalishi

Oldini olish choralari:

- Sayt manzilini diqqat bilan tekshirish (ortiqcha belgi yoki harf yo‘qligiga e’tibor berish)
- Bank xizmatlaridan faqat rasmiy mobil ilova yoki to‘g‘ridan-to‘g‘ri kiritilgan manzil orqali foydalanish
- Elektron pochta yoki messenjer orqali kelgan shubhali havolalarga kirmaslik
- Ikki bosqichli tasdiqlash funksiyasini yoqish
- Brauzerda xavfsizlik belgilariga (qulf belgisi) e’tibor qaratish

Soxta saytlar orqali aldash usuli texnik jihatdan murakkab ko‘rinsa-da, uning asosiy tayanchi foydalanuvchining e’tiborsizligi hisoblanadi. Shu sababli internetda har qanday havolaga ishonch bilan kirmaslik va rasmiy manbalargina foydalanish muhim ahamiyatga ega.

3. Telefon orqali firibgarlik va SMS orqali aldash— bu fuqarolardan shaxsiy hamda moliyaviy ma’lumotlarni qo‘lga kiritish maqsadida aloqa vositalari orqali amalga oshiriladigan jinoyat turidir. Ushbu usulda firibgarlar bevosita muloqot orqali ishonch qozonishga yoki shoshilinch vaziyat yaratishga harakat qiladi.

Telefon qo‘ng‘irog‘i orqali ma’lumotlarni so‘rab olish holatida jinoyatchi o‘zini bank xodimi, xavfsizlik xizmati vakili yoki boshqa rasmiy tashkilot nomidan tanishtiradi. Ular odatda “hisobingizdan noqonuniy pul yechishga urinish bo‘ldi”, “kartangiz bloklanmoqda” yoki “tezda tasdiqlash kerak” kabi gaplar bilan fuqaroning e’tiborini tortadi va vahima uyg‘otadi. Suhbat davomida karta raqami, amal qilish muddati, orqa tarafdagi xavfsizlik kodi yoki SMS orqali kelgan tasdiqlash kodini aytish so‘raladi.

SMS orqali aldashda esa foydalanuvchiga zararli havola yuboriladi. Xabarda “mukofot yutdingiz”, “to‘lovni qabul qiling”, “kartangiz bloklandi” kabi yolg‘on ma’lumotlar bo‘ladi. Havolaga kirilganda foydalanuvchi soxta sahifaga yo‘naltiriladi yoki zararli dastur yuklab olinishi mumkin.

Xavfi:

- Bank hisobidagi mablag‘larning noqonuniy o‘tkazilishi
- Karta ma’lumotlarining o‘g‘irlanishi
- Shaxsiy ma’lumotlarning uchinchi shaxslarga tarqalishi
- Firibgarlar tomonidan kredit rasmiylashtirilishi

Oldini olish choralari:

- Noma’lum raqamdan kelgan qo‘ng‘iroqlarga shaxsiy ma’lumot bermaslik
- Hech qachon SMS orqali kelgan tasdiqlash kodini begona shaxsga aytmaslik
- Shubhali havolalarga kirmaslik
- Rasmiy ma’lumotni faqat bankning o‘ziga mustaqil qo‘ng‘iroq qilib aniqlashtirish
- Telefon raqamni yashirin saqlash va ortiqcha joylarda qoldirmaslik

Telefon va SMS orqali amalga oshiriladigan firibgarlik usullari sodda ko‘rinsa-da, ular eng tez tarqaladigan va eng ko‘p uchraydigan tahdidlardan biri hisoblanadi. Shu sababli hushyorlik va shaxsiy ma’lumotlarni himoya qilish madaniyati muhim ahamiyat kasb etadi.

4. Zararli dasturlar— bu foydalanuvchining roziligisiz uning qurilmasiga o‘rnatilib, shaxsiy va moliyaviy ma’lumotlarni yashirin ravishda qo‘lga kiritishga mo‘ljallangan maxsus dasturiy vositalardir. Ular ko‘pincha soxta havolalar, ishonchsiz ilovalar, noma’lum fayllar yoki qalbaki dasturlar orqali tarqatiladi.

Telefon yoki kompyuterga virus joylashtirish firibgarlar tomonidan eng ko‘p qo‘llaniladigan usullardan biridir. Foydalanuvchi zararli faylni yuklab olganidan so‘ng dastur qurilmada yashirin ishlay boshlaydi. Ayrim zararli dasturlar klaviaturada terilgan ma’lumotlarni yozib boradi, boshqalari esa ekran faoliyatini kuzatishi mumkin.

Bank ilovasidagi ma’lumotlarni yashirin kuzatish orqali jinoyatchilar login, parol, karta rekvizitlari va boshqa maxfiy ma’lumotlarni qo‘lga kiritadi. Ba’zi zararli dasturlar bank ilovasining ustiga soxta oyna chiqarib, foydalanuvchidan ma’lumot kiritishni talab qiladi. Natijada kiritilgan ma’lumotlar bevosita firibgarlarga yuboriladi.

Yana bir xavfli jihat — bir martalik tasdiqlash parollarini qo‘lga kiritishdir. Ayrim zararli dasturlar SMS xabarlarni o‘qish imkoniyatiga ega bo‘lib, bankdan kelgan tasdiqlash kodlarini jinoyatchilarga yetkazadi. Bu esa hisobdan pul o‘tkazishni osonlashtiradi.

Xavfi:

- Bank hisobining to‘liq nazoratdan chiqishi
- Mablag‘larning noqonuniy o‘tkazilishi
- Shaxsiy ma’lumotlarning o‘g‘irlanishi
- Qurilmaning umumiy xavfsizligiga zarar yetishi

Oldini olish choralari:

- Ilovalarni faqat rasmiy dastur platformalaridan yuklab olish
- Noma’lum manbalardan kelgan fayllarni ochmaslik
- Qurilmaga ishonchli antivirus dasturini o‘rnatish
- Operatsion tizim va ilovalarni muntazam yangilab borish
- Bank ilovasiga kirishda qo‘shimcha himoya (barmoq izi, yuzni aniqlash) funksiyalaridan foydalanish

Zararli dasturlar texnik jihatdan murakkab tahdid bo‘lib, ko‘pincha foydalanuvchining ehtiyotsizligi sababli qurilmaga kirib boradi. Shu bois raqamli gigiyena qoidalariga amal qilish moliyaviy xavfsizlikning muhim sharti hisoblanadi.

5. Bankomat qurilmasi orqali ma’lumot ko‘chirish— bu jinoyatchilar tomonidan bankomat yoki to‘lov terminaliga maxsus yashirin moslamalar o‘rnatish orqali plastik karta ma’lumotlarini qo‘lga kiritish usulidir. Ushbu turdagi jinoyat odatda tashqi ko‘rinishda deyarli bilinmaydigan texnik qurilmalar yordamida amalga oshiriladi va foydalanuvchi ko‘pincha buni sezmay qoladi.

Eng ko‘p uchraydigan usullardan biri — bankomatning karta kiritiladigan qismiga maxsus o‘quvchi moslama o‘rnatishdir. Ushbu moslama karta magnit tasmasidagi ma’lumotlarni o‘qib, nusxalab oladi. Natijada jinoyatchilar kartaning elektron nusxasini yaratishi va undan boshqa joyda foydalanishi mumkin.

Ba’zi hollarda jinoyatchilar bankomat klaviaturasi ustiga soxta klaviatura qoplamasi o‘rnatadi yoki yashirin kamera joylashtiradi. Kamera yoki soxta qurilma orqali foydalanuvchi kiritgan maxfiy raqam (PIN-kod) yozib olinadi. Agar karta ma’lumoti va PIN-kod birgalikda qo‘lga kiritilsa, hisobdan pul yechib olish juda osonlashadi.

Ushbu turdagi jinoyatlar ko‘pincha odam kam qatnaydigan joylardagi yoki yetarlicha nazorat qilinmaydigan bankomatlarda sodir etiladi. Ayrim hollarda savdo shoxobchalaridagi to‘lov terminallariga ham noqonuniy qurilmalar o‘rnatilishi mumkin.

Xavfi:

- Kartaning soxta nusxasi tayyorlanishi
- Hisobdan naqd pul yechib olinishi
- Chet elda yoki boshqa hududda noqonuniy operatsiyalar amalga oshirilishi
- Mijoz zarar ko‘rganini kech bilishi

Oldini olish choralari:

- Bankomatdan foydalanishdan oldin karta kiritiladigan joyni va klaviaturani diqqat bilan tekshirish
- Qimirlab turadigan yoki g‘ayrioddiy ko‘rinadigan moslamalar bo‘lsa, undan foydalanmaslik
- PIN-kodni kiritayotganda klaviaturani qo‘l bilan yopib turish
- Odam gavjum va kuzatuv kameralari mavjud joylardagi bankomatlardan foydalanish
- Hisob harakatlarini muntazam nazorat qilish va shubhali operatsiya aniqlansa darhol bankka murojaat qilish

Hozirgi kunda ko‘plab banklar magnit tasma o‘rniga himoyasi kuchli mikrochipli kartalarni joriy etmoqda. Biroq ehtiyotkorlik choralariga rioya qilmaslik baribir xavf tug‘dirishi mumkin. Shuning uchun bankomatlardan foydalanishda hushyorlik va e’tibor moliyaviy xavfsizlikning muhim omili hisoblanadi.

6. SIM-kartani noqonuniy almashtirish— bu jinoyatchilar tomonidan fuqaroning mobil telefon raqamini ruxsatsiz ravishda boshqa SIM kartaga o‘tkazish orqali uning bank hisobiga kirish usulidir. Ushbu usul odatda mobil aloqa operatori tizimidan foydalanish yoki soxta hujjatlar orqali amalga oshiriladi. Natijada jabrlanuvchining telefon raqami vaqtincha o‘chib qoladi va barcha kiruvchi qo‘ng‘iroq hamda SMS xabarlar firibgarning qo‘liga o‘tadi.

Mobil raqamni boshqa SIM kartaga ruxsatsiz o‘tkazish jarayonida jinoyatchilar oldindan shaxsiy ma’lumotlarni (pasport ma’lumoti, tug‘ilgan sana va boshqalar) turli yo‘llar bilan qo‘lga kiritgan bo‘lishi mumkin. Ushbu ma’lumotlar yordamida ular mobil operatorga murojaat qilib, “SIM karta yo‘qolgan” degan bahona bilan yangi karta rasmiylashtiradi.

SMS orqali keladigan tasdiqlash kodlarini qo‘lga kiritish esa ushbu jinoyatning eng xavfli bosqichidir. Chunki bank tizimida ko‘plab operatsiyalar aynan telefon raqamiga yuboriladigan bir martalik kod orqali tasdiqlanadi. Agar ushbu kod jinoyatchi qo‘liga tushsa, u hisobdan pul o‘tkazishi, parolni almashtirishi yoki hatto kredit rasmiylashtirishi mumkin.

Ko‘pincha jabrlanuvchi telefon tarmog‘i to‘satdan ishlamay qolganida yoki “faqat favqulodda qo‘ng‘iroqlar” degan yozuv paydo bo‘lganida vaziyatdan xabardor bo‘ladi. Ammo shu vaqt ichida moliyaviy zarar yetkazilishi ehtimoli yuqori bo‘ladi.

Xavfi:

- Bank hisobiga to‘liq kirish imkoniyati yaratilishi
- Mablag‘larning tezkor o‘tkazib yuborilishi
- Parollarning o‘zgartirilishi va hisobning egasi nazoratdan chiqishi
- Kredit va boshqa majburiyatlarning rasmiylashtirilishi

Oldini olish choralari:

- Mobil raqamni pasport ma’lumotlari bilan qo‘shimcha himoya qilish
- Bank ilovasida ikki bosqichli tasdiqlashning qo‘shimcha usullarini yoqish
- Telefon tarmog‘i sababsiz o‘chib qolsa, darhol mobil operatorga murojaat qilish
- Shaxsiy ma’lumotlarni begona shaxslarga bermaslik
- Bank hisobidagi harakatlarni muntazam tekshirib borish

SIM-kartani noqonuniy almashtirish usuli texnik va tashkiliy zaifliklardan foydalanishga asoslanadi. Shu sababli mobil aloqa xavfsizligi ham moliyaviy xavfsizlikning ajralmas qismi hisoblanadi.

7. Onlayn savdo orqali firibgarlik — bu firibgarlar tomonidan internet-do‘kon yoki ijtimoiy tarmoq orqali soxta savdo platformalari yaratib, foydalanuvchilardan oldindan to‘lov olib, mahsulot yoki xizmatni yetkazmaslik orqali amalga oshiriladigan jinoyat turidir. Ushbu usul tez tarqalgan va ayniqsa internet-savdo rivojlangan zamonamizda keng tarqalgan.

Firibgarlar soxta internet-do‘kon yaratadi yoki mavjud ishonchli platformaga o‘xshash profil tashkil etadi. Do‘kon dizayni, mahsulot rasmlari va narxlari real ko‘rinishga ega bo‘ladi, bu esa foydalanuvchida ishonch uyg‘otadi. Ba’zan ular “chegirma”, “cheklangan stok”, “tezkor xarid” kabi shoshilinch e’lonlar orqali xaridorni chalg‘itadi va tez qaror qabul qilishga majbur qiladi.

Xaridor oldindan to‘lovni amalga oshirgach, firibgar mahsulotni yubormaydi yoki soxta kuzatish raqamini taqdim etadi. Shu bilan birga, firibgarlar ba’zan kartaga to‘lovni amalga oshirish uchun yolg‘on havolalar yuboradi, bu orqali karta ma’lumotlarini qo‘lga kiritadi.

Xavfi:

- Oldindan to‘langan mablag‘ning qaytarilmasligi
- Karta ma’lumotlari va shaxsiy ma’lumotlarning o‘g‘irlanishi
- Ijtimoiy tarmoqlarda firibgarlar tomonidan qo‘shimcha moliyaviy zarar yetkazilishi
- Shubhali faoliyatlar natijasida boshqa moliyaviy hujumlarga uchrash ehtimoli

Oldini olish choralari:

- Internet-do‘kon yoki ijtimoiy tarmoq sahifasining ishonchliligini tekshirish
- Faqat rasmiy, litsenziyalangan onlayn savdo platformalaridan xarid qilish
- Oldindan to‘lov qilishdan avval, sotuvchi va mahsulot haqida izlanish olib borish
- Bank kartasi ma’lumotlarini xavfsiz saqlash va begona havolalarga kiritmaslik
- Xaridlar uchun xavfsiz to‘lov tizimlaridan foydalanish (masalan, faqat rasmiy bank ilovasi yoki to‘lov servisi)

Onlayn savdo firibgarligi, foydalanuvchining e’tiborsizligi va shoshilinch qaror qabul qilishidan foydalanadi. Shu sababli onlayn xaridlarni amalga oshirishda hushyorlik va tekshiruvli yondashuv eng muhim himoya vositasidir.

8. Ochiq internet tarmoqlari orqali hujum— bu foydalanuvchi himoyasiz Wi-Fi yoki boshqa umumiy internet tarmoqlaridan foydalanganda, uning shaxsiy va moliyaviy ma’lumotlarini jinoyatchilar tomonidan o‘g‘irlanishi usulidir. Bu turdagi tahdid ayniqsa kafelar, mehmonxonalar, aeroportlar yoki jamoat joylaridagi ochiq Wi-Fi tarmoqlarida uchraydi.

Firibgarlar ushbu tarmoqlarda turli texnik vositalar yordamida ma’lumotlarni “eshitish” (sniffing) imkoniyatiga ega bo‘ladi. Masalan, foydalanuvchi bank ilovasiga kirayotganda, karta raqami, parol, tasdiqlash kodi va boshqa shaxsiy ma’lumotlar firibgarning qurilmasi orqali o‘qilishi mumkin. Ba’zi hollarda ular foydalanuvchi qurilmasiga zararli dastur yuborish orqali ham nazorat o‘rnatadi.

Ochiq tarmoqlarda login va parolni kiritish yoki onlayn to‘lovlarni amalga oshirish juda xavfli bo‘lib, foydalanuvchi sezmay turib katta moliyaviy zarar ko‘rishi mumkin.

Xavfi:

- Bank hisobidagi mablag‘larning noqonuniy o‘tkazilishi
- Karta va parol ma’lumotlarining o‘g‘irlanishi
- Shaxsiy ma’lumotlarning uchinchi shaxslarga tarqalishi
- Qurilmaga zararli dastur o‘rnatilishi

Oldini olish choralari:

- Umumiy va himoyasiz Wi-Fi tarmoqlarida bank operatsiyalarini amalga oshirmaslik
- VPN (Virtual Private Network) xizmatidan foydalanish
- Bank ilovasi va brauzerlar orqali SSL va HTTPS bilan himoyalangan saytlar orqali kirish
- Qurilmada antivirus va xavfsizlik dasturlarini o‘rnatish

- Muhim login va parollarni faqat shaxsiy qurilmada kiritish

Ochiq internet tarmoqlari orqali hujumlar foydalanuvchining ehtiyotsizligi va xavfsizlik choralariga rioya qilmasligidan foydalanadi. Shu sababli, jamoat Wi-Fi tarmoqlarida moliyaviy operatsiyalarni amalga oshirishdan saqlanish va shaxsiy himoya vositalaridan foydalanish juda muhimdir.

9. Ma'lumotlar bazasining sizib chiqishi— bu bank yoki boshqa moliyaviy tashkilotlarning ichki ma'lumotlar omboridan mijozlar haqidagi shaxsiy va moliyaviy ma'lumotlarning ruxsatsiz ravishda o'zga shaxslarga tarqalishi yoki sotilishi hodisasidir. Ushbu tahdid ko'pincha texnik zaifliklar, ichki xodimlar xato yoki firibgarlar tomonidan amalga oshiriladigan kiberhujumlar natijasida yuzaga keladi. Ma'lumotlar omboridan sizib chiqadigan ma'lumotlar quyidagilarni o'z ichiga olishi mumkin:

- Karta raqamlari, amal qilish muddati, xavfsizlik kodlari (CVV/CVC)
- Foydalanuvchi ismi va familiyasi, tug'ilgan sana, manzil
- Telefon raqami va elektron pochta manzili
- Bank hisob raqamlari va tranzaksiya tarixi

Jinoyatchilar bu ma'lumotlarni qora bozorda sotishi yoki soxta saytlar, telefon va SMS firibgarligi, onlayn savdo firibgarligi orqali qo'llashi mumkin. Misol uchun, ular karta rekvizitlarini sotib olgan firibgarlar bank hisobidan noqonuniy pul o'tkazishi yoki firibgarlik operatsiyalarini amalga oshirishi mumkin.

Ma'lumotlar bazasining sizib chiqishi ko'pincha quyidagi holatlar natijasida sodir bo'ladi:

1. **Kiberhujumlar:** Hackerlar tashkilot serverlariga kirib, ma'lumotlarni o'g'irlashadi. Bu SQL-injection, zararli dasturlar, server konfiguratsiyasidagi zaifliklar orqali amalga oshiriladi.
2. **Ichki xodimlarning xatosi yoki firibgarligi:** Ba'zi hollarda xodimlar ma'lumotlarni noto'g'ri saqlash, himoyasiz qurilmalar orqali ishlash yoki bilib turib ularga ruxsat berish orqali ma'lumotlar sizib chiqadi.
3. **Yomon tashkil etilgan xavfsizlik siyosati:** Kuchsiz parollar, eski dasturiy ta'minot, autentifikatsiya va ruxsatlar tizimidagi zaifliklar ma'lumotlar xavfsizligini buzadi.

Xavfi:

- Mijozlar shaxsiy va moliyaviy ma'lumotlarini yo'qotadi
- Bank kartalari va hisoblar firibgarlar tomonidan o'g'irlanadi
- Qora bozorda ma'lumotlar sotilishi natijasida moliyaviy zarar yuz beradi
- Ijtimoiy muhandislik va phishing hujumlari kengayadi
- Bankning obro'si va mijozlar ishonchi zarar ko'radi

Oldini olish choralari:

- Bank va moliyaviy tashkilotlarda ma'lumotlar xavfsizligi bo'yicha kuchli ichki siyosat joriy etish
- Ma'lumotlar bazalarini shifrlash va muntazam xavfsizlik tekshiruvlari o'tkazish
- Xodimlarga kiberxavfsizlik bo'yicha muntazam treninglar berish
- Faqat kuchli parollar va ikki bosqichli autentifikatsiya tizimlarini qo'llash
- Ma'lumotlarni zaxira qilish va serverlarga kirishni qat'iy nazorat qilish
- Ma'lumotlar sizib chiqqan holatda tezkor ogohlantirish va profilaktik choralarni ko'rish

Ma'lumotlar bazasining sizib chiqishi tahdidi ayniqsa katta banklar va ko'p mijozga xizmat ko'rsatuvchi tashkilotlar uchun jiddiy muammo hisoblanadi. Shu sababli, axborot xavfsizligini ta'minlash va muntazam auditlar o'tkazish har doim ustuvor vazifa bo'lishi kerak.

10. Ichki tahdidlar— bu bank, moliya tashkiloti yoki savdo shoxobchasidagi xodimlar tomonidan maxfiy ma'lumotlardan noto'g'ri foydalanish, ularni ruxsatsiz uchinchi shaxslarga berish yoki shaxsiy manfaat yo'lida ishlatish holatlarini anglatadi. Bu tahdid tashqi

kiberhujumlarga qaraganda kamroq e'tiborni tortishi mumkin, lekin xavfi juda yuqori, chunki ichki xodimlar tizim va jarayonlarni yaxshi biladi.

Ichki tahdidlarning asosiy shakllari quyidagilar:

1. **Ma'lumotlarni ruxsatsiz ko'rish yoki tarqatish:** Bank xodimi mijozlar kartalari, hisob raqamlari yoki shaxsiy ma'lumotlarni o'z manfaatiga yoki uchinchi shaxsga berish uchun foydalanadi. Bu holatda xaridorlar o'z mablag'lari va shaxsiy ma'lumotlari ustidan nazoratni yo'qotadi.
2. **Firibgarlik va o'g'irlik:** Ichki xodimlar karta ma'lumotlarini va tasdiqlash kodlarini qo'lga kiritib, hisobdan pul yechish yoki soxta tranzaksiya amalga oshirishlari mumkin. Shu yo'l bilan ular kompaniya va mijozlarga jiddiy moliyaviy zarar yetkazadi.
3. **Ichki tizimlarni suiiste'mol qilish:** Xodimlar ruxsatli tizimlardan foydalangan holda ma'lumotlarni ko'chirishi, o'zgartirishi yoki o'chirishlari mumkin. Masalan, ular firibgarlar bilan hamkorlikda soxta hisob ochish yoki mavjud ma'lumotlarni manipulyatsiya qilish orqali firibgarlik qilishi mumkin.
4. **Maxfiy ma'lumotlarni sotish:** Ichki xodimlar mijoz ma'lumotlarini qora bozorda sotishi mumkin, bu esa karta rekvizitlari va shaxsiy ma'lumotlarning noqonuniy qo'lga o'tishiga olib keladi.

Xavfi:

- Bank va mijozlar moliyaviy zarar ko'rishi
- Shaxsiy ma'lumotlarning uchinchi shaxslarga tarqalishi
- Ijtimoiy muhandislik, phishing va boshqa firibgarlik turlarining kengayishi
- Bankning obro'si va mijozlar ishonchining yo'qolishi
- Ichki nazorat tizimining zaifligi, bu kelajakda boshqa tahdidlarni ham yuzaga keltiradi

Oldini olish choralari:

- Bank va tashkilotlarda ichki xavfsizlik siyosatini kuchaytirish
- Xodimlarning ma'lumotlarga kirish huquqlarini qat'iy belgilash va cheklash
- Tizim faoliyatini muntazam audit qilish va monitoring qilish
- Shubhali harakatlarni aniqlash uchun avtomatlashtirilgan tizimlarni joriy etish
- Xodimlarga kiberxavfsizlik va axborot maxfiyligi bo'yicha doimiy treninglar berish
- Ichki tahdid aniqlangan hollarda tezkor choralar ko'rish va qonuniy javobgarlikni qo'llash

Ichki tahdidlar ko'pincha tashqi kiberhujumlarga qaraganda aniqlash qiyin, lekin ularning oqibatlari yanada jiddiy bo'lishi mumkin. Shu sababli har bir moliyaviy tashkilot uchun ichki nazorat va xodimlarning javobgarligi ustuvor ahamiyatga ega.

O'zbekiston bank tizimida plastik kartalarga tahdid soluvchi xavf-xatarlarni xavf darajasi bo'yicha reytinglangan va iqtisodiy oqibatlari

№	Tahdid turi	Xavf darajasi	Iqtisodiy oqibatlari
1	Ijtimoiy muhandislik	Juda yuqori	Mablag'larning tezkor o'g'irlanishi, mijoz ishonchi pasayishi
2	Soxta saytlar va aldovli havolalar	Yuqori	Karta ma'lumotlari oshkor bo'lishi, moliyaviy zarar
3	Zararli dasturlar	Yuqori	Karta va shaxsiy ma'lumotlar o'g'irlanishi, moliyaviy yo'qotish

4	Telefon orqali firibgarlik va SMS orqali aldash	O‘rta	Mablag‘ yo‘qotish, shaxsiy ma’lumotlarning oshkor bo‘lishi
5	Bankomat qurilmasi orqali ma’lumot ko‘chirish	O‘rta	Karta ma’lumotlari nusxalanishi, mablag‘ yo‘qotish
6	SIM-kartani noqonuniy almashtirish	O‘rta	SMS tasdiqlash kodlari o‘g‘irlanishi, mablag‘ yo‘qotish
7	Onlayn savdo orqali firibgarlik	O‘rta	Oldindan to‘lov olib, mahsulot yetkazilmasligi, mijoz ishonchi pasayishi
8	Ochiq internet tarmoqlari orqali hujum	Past	Ma’lumotlarning oshkor bo‘lishi, moliyaviy zarar
9	Ma’lumotlar bazasining sizib chiqishi	Juda yuqori	Mijoz ma’lumotlari tarqalishi, karta rekvizitlarining noqonuniy sotilishi, moliyaviy yo‘qotish
10	Ichki tahdidlar	Yuqori	Xodimlar noto‘g‘ri foydalanishi, moliyaviy va reputatsion zarar

HOZIRGI HIMOYA MEXANIZMLARI VA ULARNING SAMARADORLIGI

Hozirgi kunda O‘zbekiston bank tizimida plastik kartalar va onlayn tranzaksiyalarni himoya qilish uchun turli zamonaviy texnologiyalar keng joriy etilgan. Raqamli texnologiyalar va internet xizmatlarining jadal rivojlanishi bank xizmatlarini tez, qulay va foydalanuvchi uchun moslashtirilgan holga keltirdi. Misol uchun, mijozlar endi o‘z uylaridan chiqmasdan bank operatsiyalarini amalga oshirishi, mablag‘larni o‘tkazishi yoki kredit va depozit xizmatlaridan foydalanishi mumkin.

Biroq, ushbu texnologik rivojlanish bilan birga, bank tizimlariga tahdidlar ham keskin oshdi. Internet va raqamli xizmatlar orqali firibgarlik va kiberhujumlar sodir etish osonlashdi, chunki jinoyatchilar yangi usullar orqali mijozlarning shaxsiy va moliyaviy ma’lumotlarini qo‘lga kiritishga harakat qilmoqda. Shu bilan birga, jismoniy kartalar, bankomatlar, to‘lov terminallari va mobil ilovalardan foydalanish davomida ichki va tashqi tahdidlar yuzaga kelmoqda. Shuning uchun, O‘zbekiston bank tizimida plastik kartalar va onlayn tranzaksiyalarni himoya qilishda ko‘p qatlamli xavfsizlik yondashuvi qo‘llaniladi. Bu yondashuv quyidagi asosiy maqsadlarni o‘z ichiga oladi:

1. **Mijoz mablag‘larini himoya qilish:** Har bir tranzaksiya xavfsiz tarzda amalga oshiriladi va firibgarlik ehtimoli minimal darajada bo‘ladi.
2. **Texnologik himoya vositalarini birlashtirish:** bir martalik parol, uch bosqichli autentifikatsiya, biometrik identifikatsiya, tranzaksiya monitoringi kabi texnologiyalar bir-birini to‘ldiradi.

3. **Ichki va tashqi tahdidlarga qarshi himoya:** Bank tizimi nafaqat kiberhujumlar, balki ichki xodimlar yoki ichki tizim xatolaridan kelib chiqadigan tahdidlarga qarshi ham choralar ko‘radi.
4. **Mijozlarni moliyaviy savodxonlikka o‘rgatish:** Banklar foydalanuvchilarga ehtiyotkorlik va xavfsizlik qoidalarini tushuntirib, ularni firibgarlik va kiberhujumlardan himoya qilishga o‘rgatadi.

Shu bilan birga, banklar xavfsizlik tizimlarini doimiy ravishda yangilab, yangi texnologiyalarni tatbiq etadi va mavjud himoya vositalarining samaradorligini oshirishga harakat qiladi. Bu jarayon mijozlar uchun qulay, ishonchli va xavfsiz bank xizmatlarini ta’minlaydi. Natijada, zamonaviy himoya mexanizmlari faqat texnologiyaga tayanmay**,** balki mijoz ehtiyotkorligi va ichki xavfsizlik choralarini ham birlashtirib, kompleks yondashuv orqali ishlaydi. Shu yondashuv orqali bank tizimi har xil tahdidlarga tayyor bo‘lib, firibgarlik va kiberhujumlar xavfini minimal darajaga tushiradi.

Hozirgi kunda O‘zbekiston bank tizimida plastik kartalar va onlayn tranzaksiyalarni himoya qilish uchun eng keng tarqalgan xavfsizlik mexanizmlari quyidagilar:

1. **Bir martalik parol** – SMS yoki mobil ilova orqali yuboriladigan yagona tranzaksiya kodi.
2. **Uch bosqichli autentifikatsiya** – karta yoki token, parol yoki PIN va biometrik tasdiqlashni birlashtiradi.
3. **Biometrik autentifikatsiya** – barmoq izi, yuzni aniqlash, ovoz orqali tasdiqlash.
4. **Tranzaksiyalar monitoringi** – shubhali operatsiyalarni real vaqt rejimida aniqlash va bloklash tizimlari.
5. **Soxta sayt va aldovli havolalar filtrasi** – rasmiy bank saytlariga o‘xshash qalbaki saytlarni aniqlash va bloklash.
6. **Ma’lumotlarni shifrlash** – onlayn tranzaksiyalar va ma’lumot uzatishni xavfsiz qilish.
7. **Bank ilovalaridagi xavfsizlik tokenlari** – mobil ilovalar orqali tranzaksiya tasdiqlash.
8. **Cheklangan tranzaksiya limiti** – katta summali operatsiyalarni qo‘shimcha tasdiqlash bilan amalga oshirish.
9. **Ichki xavfsizlik tizimi** – xodimlarning ma’lumotlarga kirish huquqlari, audit va nazorat tizimi.
10. **Xavfsiz tarmoqlar va VPN -“Virtual Shaxsiy Tarmoq” tavsiyalari** – jamoat tarmoqlarida bank xizmatlaridan foydalanishda qo‘llaniladigan himoya chorasi.

O‘zbekiston bank tizimidagi plastik kartalarni himoya qiluvchi asosiy mexanizmlarning samaradorligi va cheklovlari

№	Himoya mexanizmi	Afzalliklari	Cheklovlari	Samaradorlik
1	**Bir martalik parol**	Har bir tranzaksiya uchun yagona kod	SMS o‘g‘irlanishi mumkin	Oddiy hujumlarga qarshi samarali
2	**Uch bosqichli autentifikatsiya**	Bir nechta qatlam, yuqori xavfsizlik	Murakkab, barcha mijozlar uchun qiyin	Yuqori xavfsizlik
3	**Biometrik autentifikatsiya**	Qulay, parolni eslab qolish shart emas	Qurilma moslashuvi, ma’lumot o‘g‘irilsa qayta tiklash qiyin	Yuqori xavfsizlik

4	**Tranzaksiyalar monitoringi**	Shubhali operatsiyalarni tez aniqlash	False positive, kichik firibgarlikni aniqlash qiyin	Umumiy xavfsizlikni oshiradi
5	**Soxta sayt va havolalar filtrasi**	Qalbaki saytlarni bloklaydi	Yangi qalbaki saytlarni aniqlash qiyin	Phishing xavfini kamaytiradi
6	**Shifrlash**	Ma'lumot uzatishni xavfsiz qiladi	Eskirsa xavf mavjud	Onlayn ma'lumotni himoyalaydi
7	**Bank ilovalaridagi token**	Qo'shimcha himoya qatlamini yaratadi	Qurilma yo'qolsa tranzaksiya bo'lmaydi	Onlayn tranzaksiyalarni himoyalaydi
8	**Cheklangan tranzaksiya limiti**	Katta summali operatsiyalarni tekshiradi	Kichik firibgarlikni aniqlay olmaydi	Katta firibgarliklarni kamaytiradi
9	**Ichki xavfsizlik tizimi**	Xodim nazoratini kuchaytiradi	Ichki firibgarlikni 100% oldini olish qiyin	Ichki tahdidlarga qarshi samarali
10	**Xavfsiz tarmoqlar va VPN**	Jamoat tarmoqlarida xavfsiz foydalanish	Noto'g'ri sozlansa xavfsizlik past bo'ladi	Umumiy Wi-Fi xavfini kamaytiradi

KIBERXAVFSIZLIKNI TAKOMILLASHTIRISH YO'LLARI

Hozirgi kunda O'zbekiston bank tizimida plastik kartalar va onlayn tranzaksiyalar sonining keskin ortishi bilan birga, kiberhujumlar va firibgarliklar xavfi ham sezilarli darajada oshmoqda. Raqamli texnologiyalar va internet xizmatlarining jadal rivojlanishi bank operatsiyalarini qulay, tezkor va foydalanuvchilar uchun moslashtirilgan holga keltirgan bo'lsa-da, shu bilan birga jinoyatchilar yangi usullar orqali mijozlarning shaxsiy va moliyaviy ma'lumotlarini qo'lga kiritish imkoniyatiga ega bo'lmoqda. Shu sababli bank tizimini himoya qilish va mijoz mablag'larini saqlash maqsadida kiberxavfsizlikni takomillashtirish bo'yicha kompleks choralar joriy etilishi muhim hisoblanadi. Ushbu choralar nafaqat texnologik himoyani, balki foydalanuvchi ehtiyotkorligini va ichki xavfsizlikni ham o'z ichiga oladi.

Quyida asosiy yo'nalishlar kengaytirilgan holda keltiriladi:

1. Ko'p bosqichli autentifikatsiya- Ko'p bosqichli autentifikatsiya bank tizimida xavfsizlikni mustahkamlashning samarali usulidir. Bu jarayon foydalanuvchining shaxsini tasdiqlashda SMS orqali yuboriladigan tasdiqlash kodi, mobil ilova orqali qo'shimcha tasdiqlash va biometrik tekshiruvni, masalan, barmoq izi yoki yuzni aniqlashni birlashtiradi. Bu usul tranzaksiyalarni himoyalashda juda samarali bo'lib, karta yoki parol o'g'irlangan holatlarda ham mablag'larning xavfsizligini ta'minlaydi. Shu bilan birga, foydalanuvchi uchun qulaylik yaratadi, chunki biometrik tasdiqlash orqali tranzaksiya tez va sodda amalga oshiriladi. Katta summali yoki onlayn xaridlar uchun ko'p bosqichli autentifikatsiyani majburiy qilish va foydalanuvchilarga ushbu tizimdan to'g'ri foydalanish bo'yicha o'qitish tavsiya etiladi.

2. Sun'iy intellekt asosida shubhali operatsiyalarni aniqlash- Sun'iy intellekt asosida shubhali operatsiyalarni aniqlash tizimi foydalanuvchining odatiy xarid xatti-harakatini kuzatadi va odatdagidan farq qiladigan tranzaksiyalarni real vaqt rejimida aniqlaydi. Shu tarzda, shubhali operatsiyalar avtomatik tarzda bloklanadi va firibgarlik ehtimoli sezilarli darajada kamayadi. Sun'iy intellekt yordamida katta miqdordagi operatsiyalar tezkor tahlil qilinadi, bu esa xavfni kamaytirishga xizmat qiladi. Shu bilan birga, algoritmlar muntazam yangilanib turishi va natijalar xavfsizlik xodimlari bilan uyg'un

ishlatilishi muhimdir. Misol uchun: 2025-yilning aprel oyida «AgroBank» mijozi kartasidan katta summa to‘lov amalga oshirilmoqchi bo‘ldi. Tranzaksiya odatdagi xaridlaridan ancha farq qilar ekan: u ilgari ishlatilmagan onlayn do‘kon — TechStore.uz dan katta miqdorda elektronik mahsulot sotib olish uchun yuborilgan edi.

Bankning sun’iy intellekt asosidagi xavfsizlik tizimi bu operatsiyani shubhali deb belgiladi, chunki mijoz so‘nggi 6 oy davomida shunga o‘xshash xaridlarni amalga oshirmagan, tranzaksiyaning summasi esa odatdagidan ancha yuqori edi. Tizim xavf reytingi yuqori deb baholagach, bu tranzaksiyani avtomatik tarzda blokladi va mijozga SMS/xabar orqali ogohlantirish yubordi. Shundan so‘ng «AgroBank» xavfsizlik bo‘limi xodimi mijoz bilan bog‘landi va operatsiya haqidagi shubhali tranzaksiya haqida tushuntirish berdi. Mijoz o‘zi bu to‘lovni amalga oshirmoqchi emasligini aytib, firibgarlik holati haqida xabar berdi. Natijada mijozning mablag‘lari yo‘qotilishining oldi olindi va shubhali hisoblangan tranzaksiya butunlay bekor qilindi. Bu holat sun’iy intellekt va monitoring tizimlarining real vaziyatlarda qanday xavfni aniqlab, oldini olishi mumkinligini aniq ko‘rsatadi.

3. Real vaqt rejimida xavflarni monitoring qilish- Real vaqt rejimida xavflarni monitoring qilish tizimi bank tranzaksiyalarini doimiy nazorat qiladi. Agar shubhali harakat aniqlansa, tizim darhol ogohlantiradi va kerak bo‘lsa tranzaksiyani bloklaydi. Bu bank va mijozlarni moliyaviy zararidan himoya qiladi. Shu bilan birga, ichki tahdidlarni aniqlash va nazorat qilish imkoniyati mavjud bo‘ladi. Kichik summali firibgarliklarni aniqlashga imkon beradigan murakkab algoritmlardan foydalanish va avtomatik monitoring tizimi bilan xodimlar nazoratini uyg‘unlashtirish tavsiya etiladi.

4. Bank va davlat organlari o‘rtasida axborot almashuvini kuchaytirish- Bank va davlat organlari o‘rtasida axborot almashuvini kuchaytirish ham muhim yo‘ldir. Tezkor axborot almashuvi kiberjinoyatlar va firibgarliklarni tez aniqlashga yordam beradi, jinoyatchilar faoliyatini kuzatish va qonuniy choralar ko‘rishga imkon yaratadi. Shu bilan birga, bank va davlat xavfsizlik tizimi o‘rtasidagi hamkorlik kuchayadi. Axborot almashuvini real vaqt rejimida amalga oshirish va kiberxavfsizlik bo‘yicha hamkorlik protokollarini ishlab chiqish va tatbiq etish tavsiya etiladi.

5. Fuqarolarni moliyaviy va kiberxavfsizlik bo‘yicha savodxonligini oshirish- Fuqarolarni moliyaviy va kiberxavfsizlik bo‘yicha savodxonligini oshirish ham katta ahamiyatga ega. Texnologik himoya vositalari samarali bo‘lsa-da, foydalanuvchining bilim darajasi va ehtiyotkorligi ham xavfsizlikni ta’minlashda muhim rol o‘ynaydi. Fuqarolar o‘z mablag‘larini himoya qilishga qodir bo‘ladi, bank tizimlariga bo‘lgan ishonch oshadi va ijtimoiy muhandislik yoki aldovli xabarlar ta’siri kamayadi. Shu maqsadda seminarlar, treninglar va elektron qo‘llanmalar orqali muntazam ta’lim berish, ochiq Wi-Fi tarmoqlarida ehtiyotkor bo‘lish, shubhali havolalarga bosmaslik va kuchli parollardan foydalanish bo‘yicha ko‘rsatmalar berish tavsiya etiladi. Bundan tashqari, maktab va universitetlarda yoshlar uchun kiberxavfsizlik bo‘yicha o‘quv dasturlarini joriy etish ham foydali bo‘ladi.

Quyidagi amaliy tavsiyalar fuqarolar xavfsizligini oshirishda muhim hisoblanadi:

1. **Parolni kuchaytirish va muntazam yangilash**
   - Plastik karta va bank ilovalariga kirishda murakkab, kamida 8–12 belgidan iborat parollardan foydalanish.
   - Parollarda harflar, raqamlar va maxsus belgilar aralashmasini qo‘llash.
   - Parollarni muntazam yangilab turish va bir xil parollarni turli xizmatlarda ishlatmaslik.
2. **Shubhali havolalarga bosmaslik**
   - SMS, elektron pochta yoki messenjerlarda kelgan noma’lum havolalarga hech qachon bosmaslik.

- Bank xodimlari hech qachon foydalanuvchidan karta raqami yoki tasdiqlash kodini so‘ramaydi, shuning uchun bunday so‘rovga javob bermaslik.

3. **Ochiq Wi-Fi tarmoqlarida ehtiyotkor bo‘lish**
   - Jamoat Wi-Fi tarmoqlarida bank ilovalari yoki onlayn to‘lov tizimlaridan foydalanmaslik.
   - Zarurat bo‘lsa, VPN xizmatidan foydalanib, ma’lumotlarni shifrlash.
4. **Ikki faktorli autentifikatsiyadan foydalanish**
   - Har bir tranzaksiya yoki kirish jarayonida ikki faktorli tasdiqlashni yoqish: SMS kod, mobil ilova orqali kod yoki biometrik tekshiruv.
   - Bu mablag‘larni qo‘shimcha himoya qilish imkonini beradi.
5. **Seminarlar, elektron qo‘llanmalar va o‘quv dasturlari orqali savodxonlikni oshirish**
   - Banklar va davlat organlari tomonidan tashkil etilgan treninglar va seminarlar orqali kiberxavfsizlik bo‘yicha muntazam ta’lim olish.
   - Maktab va universitetlarda yoshlar uchun kiberxavfsizlik bo‘yicha o‘quv dasturlarini joriy etish.
   - Elektron qo‘llanmalar va vebinarlar orqali shubhali xatti-harakatlarni aniqlash va ulardan saqlanish bo‘yicha ko‘rsatmalar berish.

Fuqarolar ushbu tavsiyalarga rioya qilganda, nafaqat o‘z mablag‘larini himoya qiladi, balki bank tizimlarida firibgarlik va kiberxavfning umumiy darajasini kamaytirishga ham hissa qo‘shadi. Shu bilan birga, moliyaviy savodxonlik va ehtiyotkorlik mijozning ishonch darajasini oshiradi va bank xizmatlaridan qulay va xavfsiz foydalanish imkonini yaratadi.

Ushbu kompleks chora-tadbirlar birgalikda qo‘llanilganda, O‘zbekiston bank tizimida plastik kartalar va onlayn tranzaksiyalarni himoya qilish darajasi sezilarli darajada oshadi va kiberfiribgarlik xavfi minimal darajaga tushadi. Shu bilan birga, mijozlar moliyaviy xavfsizlikdan to‘liq foydalanishi va bank xizmatlaridan ishonch bilan foydalana olishi mumkin bo‘ladi.

XULOSA

O‘zbekiston bank tizimida plastik kartalar va onlayn tranzaksiyalar jadal rivojlanib borayotgan bir paytda, ularni tahdid qiluvchi xavflar ham dolzarb masalaga aylanishi tabiiy jarayon. Tadqiqot natijalari shuni ko‘rsatadiki, eng xavfli tahdidlar — ijtimoiy muhandislik, soxta saytlar va zararli dasturlar — nafaqat mijoz mablag‘lariga sezilarli zarar yetkazishi, balki shaxsiy va moliyaviy ma’lumotlarning oshkor bo‘lishi, bank tizimlariga bo‘lgan ishonchning pasayishi va moliyaviy operatsiyalarga shubha bilan qarashga olib kelishi mumkin. Shu sababli, plastik kartalar xavfsizligini ta’minlash nafaqat texnik vositalarga, balki foydalanuvchi ehtiyotkorligi va tizimli nazoratga ham bog‘liqdir.

Hozirgi kunda banklar tomonidan joriy etilgan himoya mexanizmlari — bir martalik parol, uch bosqichli autentifikatsiya, biometrik tekshiruv, tranzaksiyalar monitoringi, shuningdek, ma’lumotlarni shifrlash va soxta saytlarni aniqlash tizimlari — bir-birini to‘ldiruvchi vositalar sifatida ishlaydi va umumiy xavfsizlik darajasini sezilarli oshiradi. Shu bilan birga, har bir mexanizmning o‘z cheklovlari mavjud: masalan, bir martalik parollar ijtimoiy muhandislik usullaridan kelib chiqadigan xavflarni to‘liq bartaraf eta olmaydi, monitoring tizimlari kichik firibgarliklarni aniqlashda ba’zan yetarlicha samarali bo‘lmasligi mumkin, biometrik autentifikatsiya esa texnologik cheklovlar va foydalanuvchi qulayligi bilan bog‘liq muammolarni yuzaga keltiradi.

Kiberxavfsizlikni yanada mustahkamlash uchun kompleks yondashuv zarur. Bunga ko‘p bosqichli autentifikatsiya tizimlarini keng qo‘llash, sun’iy intellekt yordamida shubhali tranzaksiyalarni aniqlash va reytinglash, real vaqt rejimida monitoring o‘rnatish, banklar va davlat organlari o‘rtasida tezkor axborot almashuvini tashkil etish hamda fuqarolarning moliyaviy va kiberxavfsizlik bo‘yicha savodxonligini oshirish kiradi. Masalan, sun’iy intellekt tizimi foydalanuvchining odatiy xarid xatti-harakatidan chetga chiqadigan tranzaksiyani

avtomatik aniqlab bloklashi, shubhali operatsiyalarni tezkor ravishda to‘xtatishi va xavfni minimallashtirishi mumkin.

Mijozlar ham o‘z mablag‘larini himoya qilishda faol rol o‘ynashi lozim. Bu parollarni kuchaytirish va muntazam yangilash, shubhali havolalarga bosmaslik, ochiq Wi-Fi tarmoqlarida ehtiyotkor bo‘lish, ikki faktorli autentifikatsiyadan foydalanish, shuningdek, seminarlar, elektron qo‘llanmalar va maktab hamda universitet dasturlari orqali muntazam ta’lim olish orqali amalga oshiriladi.

Ushbu kompleks choralar birgalikda qo‘llanilganda, O‘zbekiston bank tizimida plastik kartalar va onlayn tranzaksiyalar xavfsizligi sezilarli darajada mustahkamlanadi, kiberfiribgarlik ehtimoli kamayadi va mijozlar moliyaviy xizmatlardan ishonch bilan foydalanish imkoniyatiga ega bo‘ladi. Shu bilan birga, tizimning barqarorligi va foydalanuvchilar ishonchi oshadi, bu esa raqamli iqtisodiyotning barqaror rivojlanishiga ham xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Abdullayev, M. ***Raqamli bank xizmatlarida kiberxavfsizlik muammolari***. Toshkent: Iqtisodiyot nashriyoti, 2023.
2. Akbarova, Z. ***Onlayn tranzaksiyalar xavfsizligi: tahdidlar va yechimlar***. Journal of Security and Finance, 2024
3. Bank for International Settlements. ***Moliyaviy sektor kiberbardoshliligi.*** Basel: BIS Publications, 2022.
4. Central Bank of Uzbekistan. ***2024-yil yillik hisobot: To‘lovlar va zamonaviy bank xavfsizligi.*** Toshkent: O‘zbekiston Markaziy banki, 2025.
5. Karimov, D. ***Kiberfiribgarlik va moliyaviy xizmatlar: tahlil va profilaktika***. Toshkent: Universitet nashriyoti, 2024.
6. National Research Council. ***Raqamli to‘lov tizimlari va xavfsizlik.*** Washington, D.C.: NRC Press, 2021.
7. OECD. ***Raqamli to‘lovlarning kiberxavfsizligini oshirish.*** Parij: OECD Publishing, 2023.
8. Smith, J. & Lee, K. ***Firibgarlikni aniqlashda sun’iy intellekt.*** International Journal of Financial Technology, 2025
9. World Bank. ***Raqamli xavfsiz to‘lovlar bo‘yicha qo‘llanma.*** Washington, D.C.: World Bank, 2022.
10. Zokirov, S., & Rakhmonova, F. ***Biometrik autentifikatsiya va uning bank tizimidagi o‘rni.*** Security Technology Review, 2024

Internet manbalari

1. **US-CERT (Cybersecurity & Infrastructure Security Agency)** – kiberxavfsizlik bo‘yicha yo‘riqnomalar, ogohlantirishlar va tavsiyalar. https://www.cisa.gov/uscert
2. **Europol – Cybercrime** – Yevropa Ittifoqi kiberjinoyatlari va ularni oldini olish bo‘yicha rasmiy sahifa. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
3. **Federal Trade Commission (FTC) – Consumer Information: Scams & Safety** – firibgarlik va xavfsizlik bo‘yicha turli yo‘riqnomalar. https://www.consumer.ftc.gov/features/scam-alerts

4. **Krebs on Security** – kiberxavfsizlik bo‘yicha ekspert Brian Krebsning maxsus blogi (firibgarliklar va zaifliklar tahlili). https://krebsonsecurity.com
5. **OWASP (Open Web Application Security Project)** – veb-ilovalar xavfsizligi bo‘yicha global jamoa va himoya tavsiyalari. https://owasp.org