O'ZBEKISTON RESPUBLIKASI
ADLIYA VAZIRLIGIDA
DAVLAT RO'YXATIDAN O'TKAZILDI
RO'YXAT RAQAMI: 3759
2026 - yil 21 - Yanvar

O‘ZBEKISTON RESPUBLIKASI MARKAZIY BANKI BOSHQARUVINING QARORI

Kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari tomonidan jismoniy shaxslarga masofadan moliyaviy xizmatlar ko‘rsatishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda frod holatlarining oldini olish bo‘yicha minimal talablar to‘g‘risidagi nizomni tasdiqlash haqida

O‘zbekiston Respublikasining “O‘zbekiston Respublikasining Markaziy banki to‘g‘risida”gi Qonuniga muvofiq O‘zbekiston Respublikasi Markaziy banki boshqaruvi **qaror qiladi:**

1. Kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari tomonidan jismoniy shaxslarga masofadan moliyaviy xizmatlar ko‘rsatishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda frod holatlarining oldini olish bo‘yicha minimal talablar to‘g‘risidagi nizom ilovaga muvofiq tasdiqlansin.

2. Mazkur qaror O‘zbekiston Respublikasi Bosh prokuraturasi, Davlat xavfsizlik xizmati, Raqamli texnologiyalar vazirligi va Ichki ishlar vazirligi bilan kelishilgan.

3. Mazkur qaror rasmiy e’lon qilingan kundan e’tiboran uch oydan keyin kuchga kiradi.

O‘zbekiston Respublikasi
Markaziy banki Raisi

ISHMETOV TIMUR
AMINDJANOVICH

23-Dekabr 2025-yil
35/14 son

Kelishildi:

O'zbekiston Respublikasi Bosh prokurori 01-Dekabr 2025-yil		YO‘LDOSHEV NIG‘MATILLA TO‘LQINOVICH
Vazir 29-Noyabr 2025-yil		SHERMATOV SHERZOD XOTAMOVICH
Vazir 27-Noyabr 2025-yil		TASHPULATOV AZIZ ANVAROVICH
O`zbekiston Respublikasi DXX Raisi 20-Noyabr 2025-yil		KURBANOV BAXODIR NIZAMOVICH

O‘zbekiston Respublikasi Markaziy banki boshqaruvining 2025-yil
23-dekabrdagi 35/14-son qaroriga
ILOVA

Kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari tomonidan jismoniy shaxslarga masofadan moliyaviy xizmatlar ko‘rsatishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda frod holatlarining oldini olish bo‘yicha minimal talablar to‘g‘risidagi

NIZOM

Mazkur Nizom kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari tomonidan jismoniy shaxslarga masofadan moliyaviy xizmatlar ko‘rsatishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda frod holatlarining oldini olish bo‘yicha minimal talablarni belgilaydi.

1-bob. Umumiy qoidalar

1. Mazkur Nizomda belgilangan talablar minimal hisoblanib, kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari o‘zining ichki qoidalariga asosan o‘z mijozlarini frod holatlaridan himoya qilish bo‘yicha qo‘shimcha tashkiliy va texnik chora-tadbirlarni amalga oshirishi mumkin.

2. Ushbu Nizomda quyidagi asosiy tushunchalar qo‘llaniladi:

axborot xavfsizligi – axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holati;

autentifikatsiya – foydalanuvchi, dastur, qurilma yoki ma’lumotlarning haqiqiyligini tasdiqlash tartib-taomili;

biometrik identifikatsiya – bitta jismoniy shaxs bilan bog‘langan biometrik identifikator(lar)ni topish va qaytarish uchun biometrik ro‘yxatga olishlar ma’lumotlar bazasidan qidirish jarayoni;

frod holatlari – axborot texnologiyalaridan foydalanib sodir etilgan firibgarlik va (yoki) o‘g‘rilik holatlari;

hisobga olish yozuvi (akkaunt) – foydalanuvchining axborot tizimidagi shaxsiy qaydnomasi. U foydalanuvchiga tizimdagi ma’lum resurslar va xizmatlardan foydalanish

imkoniyatini beradi;

identifikator – obyektni tavsiflovchi va uni boshqa ko‘plab obyektlar orasida ajratib ko‘rsatish imkonini beruvchi kod yoki ramziy nom;

identifikatsiya – foydalanuvchilarning shaxsini aniqlash maqsadida ularga identifikator (noyob nomlar) tayinlash yoki tayinlangan identifikatorlarni (noyob nomlar) identifikatorlar ro‘yxati bilan solishtirish;

kiberxavfsizlik – kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati;

onlayn kredit (mikroqarz) – kredit tashkilotlari tomonidan jismoniy shaxs bo‘lgan qarz oluvchiga to‘lovlilik, muddatlilik va qaytarish shartlari asosida masofadan moliyaviy xizmatlarni ko‘rsatuvchi axborot tizimlari orqali beriladigan pul mablag‘lari;

OTP kod (One-Time Password) – bu foydalanuvchining shaxsini identifikatsiya qilish yoki autentifikatsiyadan o‘tkazish jarayonida qo‘llaniladigan, faqat bitta autentifikatsiya sessiyasi yoki amaliy operatsiya uchun mo‘ljallangan, avtomatik tarzda yaratiladigan bir martalik tasdiqlash kodi;

PUSH-xabar – foydalanuvchining mobil ilovasiga avtomatik ravishda to‘g‘ridan to‘g‘ri yuboriladigan xabar;

sessiya – foydalanuvchining tizim, dastur yoki veb-sayt bilan o‘zaro aloqada bo‘lgan vaqt oralig‘i;

SDK (Software Development Kit) – bu muayyan operatsion tizim, dasturiy muhit yoki xizmat bilan integratsiyalashgan holda yangi dasturiy mahsulotlar (ilovalar, funksiyalar yoki modullar)ni ishlab chiqish, test qilish va integratsiyalash imkonini beruvchi dasturiy vositalar, kutubxonalar, interfeyslar (API), hujjatlar, namunaviy kodlar va boshqa yordamchi resurslar majmuasidan iborat to‘plam;

masofadan moliyaviy xizmatlar ko‘rsatish – kredit va to‘lov tashkilotlari tomonidan jismoniy shaxslarga masofadan moliyaviy xizmatlarni ko‘rsatuvchi axborot tizimlari (mobil ilovalar, veb-resurs va boshqalar) orqali naqd pulsiz shaklda moliyaviy xizmatlarni taqdim etish jarayoni.

3. Kredit va to‘lov tashkilotlari masofadan moliyaviy xizmatlar ko‘rsatishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda frod holatlarining oldini olish bo‘yicha qonunchilikda belgilangan talablarning buzilish holatlari to‘g‘risida O‘zbekiston Respublikasi Markaziy bankiga (bundan buyon matnda Markaziy bank deb yuritiladi) zudlik bilan yozma yoki elektron shaklda ma’lumot berishi lozim.

4. Kredit va to‘lov tashkilotlari yangi masofadan moliyaviy xizmatlarni ko‘rsatuvchi axborot tizimini kiberxavfsizlik talablariga muvofiqligi yuzasidan qonunchilikda belgilangan tartibda ekspertizadan o‘tkazishi lozim.

Kredit va to‘lov tashkilotlarining axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati olingan ekspertiza xulosasi asosida masofadan moliyaviy xizmatlarni ko‘rsatuvchi axborot tizimining kiberxavfsizlikni ta’minlashga doir tavakkalchiliklarni baholashi hamda ijobiy natijaga erishganidan keyin amaliyotga joriy etishi shart.

2-bob. Foydalanuvchini identifikatsiya va autentifikatsiya qilish

5. Kredit va to‘lov tashkilotlari masofadan moliyaviy xizmatlarni ko‘rsatuvchi axborot tizimlari, veb-resurslar va mobil ilovalarida foydalanuvchilarni ro‘yxatdan o‘tkazish jarayonida quyidagi talablarga rioya etishlari shart:

foydalanuvchini ro‘yxatdan o‘tkazish va bank kartasini mobil ilovaga biriktirish jarayonlarini alohida autentifikatsiya orqali amalga oshirish;

foydalanuvchining telefon raqami va jismoniy shaxsning shaxsiy identifikatsiya raqami (bundan buyon matnda JSHSHIR deb yuritiladi) mos kelishini tekshirish, moslik aniqlanmagan taqdirda mobil ilovada ro‘yxatdan o‘tkazish va (yoki) bank kartasini biriktirishga yo‘l qo‘ymaslik hamda bu haqda foydalanuvchiga SMS-xabarnoma orqali xabar yuborish;

foydalanuvchi tizimda ro‘yxatdan o‘tgandan so‘ng mobil ilovadagi hisobga olish yozuviga (akkauntga) login va parolni qaytadan terib, telefon raqamiga yuborilgan OTP kodni kiritgan holda autentifikatsiyadan o‘tishini ta’minlash;

foydalanuvchining hisobga olish yozuvi (akkaunti) tizimda ro‘yxatdan o‘tgandan so‘ng, foydalanuvchining faol sessiyasi hisobga olish yozuvidan (akkauntdan) chiqarib yuborilishi va foydalanuvchi mobil ilovaga bank kartasini alohida OTP-kodni kiritib, biometrik identifikatsiyadan o‘tgan holda biriktirishini ta’minlash;

foydalanuvchining telefon raqami va u biriktirmoqchi bo‘lgan bank kartasining SMS-xabarnoma xizmatiga ulangan telefon raqami bir-biridan farq qilganda bank kartasini biriktirish jarayonini to‘xtatish va mobil ilovada foydalanuvchiga mazkur holat to‘g‘risida PUSH-xabar yuborish;

OTP kodining belgilari soni 6 tadan kam bo‘lmasligi, raqamlar va lotin alifbosidagi xarflar birikmasidan iborat bo‘lishi (A–Z, a–z, 0–9), amal qilish muddati 59 soniyadan oshmasligi hamda u 3 marotaba noto‘g‘ri kiritilganda avtomatik tarzda o‘z kuchini yo‘qotishini ta’minlash;

OTP kodni 3 marotaba noto‘g‘ri kiritgan foydalanuvchining tizimdagi harakatlarini 15 daqiqa davomida vaqtincha cheklash, keyingi cheklovlarni ichki qoidalardan kelib chiqib belgilash hamda holat haqida foydalanuvchiga SMS-xabarnoma orqali xabar berish.

6. Kredit va to‘lov tashkilotlari foydalanuvchilarni masofadan biometrik identifikatsiyadan o‘tkazishda hayotiylik faktorlarini (liveness detection) aniqlash funksiyasiga ega hamda ushbu funksiyasi real vaqt rejimida faol ishlaydigan biometrik identifikatsiya tizimidan foydalanishlari shart.

Kredit va to‘lov tashkilotlari masofadan moliyaviy xizmatlarni ko‘rsatuvchi axborot tizimlariga kirish uchun foydalanuvchilarni masofadan biometrik identifikatsiyadan o‘tkazish vazifasini mazkur faoliyat bilan shug‘ullanuvchi tashkilotlarga topshirgan taqdirda ular bilan tuziladigan shartnomalarga ushbu tashkilotlarning axborot tizimida yuzaga kelgan zaiflik yoki nosozliklar oqibatida foydalanuvchilarga yetkazilgan moddiy zararlar ularning hisobidan qoplanishiga doir talablarni kiritishi lozim.

7. Mobil ilovada ro‘yxatdan o‘tgan foydalanuvchi hisobga olish yozuviga (akkauntga) faqat ushbu shaxsga (yaqin qarindoshlarni istisno qilgan holda) tegishli bo‘lgan bank hisobvarag‘i, bank kartasi va elektron hamyonlarni biriktirishga hamda ushbu hisobga olish yozuvi (akkaunt) orqali jismoniy shaxslar o‘rtasida naqd pulsiz o‘tkazmalarni (bundan buyon matnda P2P o‘tkazmalar deb yuritiladi) amalga oshirishga ruxsat beriladi.

Bunda, yaqin qarindoshlarga qarindosh yoki quda tomondan qarindosh bo‘lgan shaxslar, ya’ni ota-ona, tug‘ishgan va o‘gay aka-uka va opa-singillar, er-xotin, farzand, shu jumladan farzandlikka olinganlar, bobo, buvi, nevaralar, shuningdek er-xotinning ota-onasi, tug‘ishgan va o‘gay aka-uka va opa-singillari kiradi.

8. Barcha P2P o‘tkazmalari OTP kod bilan tasdiqlangan holda amalga oshirilishi lozim. Veb-saytlar orqali P2P o‘tkazmalarni amalga oshirish mumkin emas.

9. Onlayn kredit (mikroqarz) va omonatlar bilan bog‘liq operatsiyalar hamda P2P o‘tkazmalarini tasdiqlash uchun yuboriladigan OTP kodlar foydalanuvchining ro‘yxatdan (autenfikatsiyadan) o‘tgan, OTP kod kelib tushgan qurilmasida amal qilishi va boshqa qurilmalarda qo‘llanishining oldi olinishi lozim.

10. Mavjud hisobga olish yozuviga (akkauntga) kirish, parolini tiklash yoki boshqa qurilmadan kirish, ro‘yxatdan o‘tish va bank kartasini biriktirish jarayonlari faqatgina biometrik identifikatsiyadan o‘tgan holda amalga oshirilishi lozim.

11. Mavjud hisobga olish yozuviga (akkauntga) boshqa qurilmadan kirish yoki uning parolini qayta tiklash jarayonida ushbu akkauntga bog‘langan barcha bank kartalari mobil ilovadan avtomatik tarzda chiqarib yuborilishi hamda ushbu qurilmada bank kartalari bo‘yicha moliyaviy operatsiyalar tarixi o‘chirib yuborilishi lozim.

Bunda mavjud hisobga olish yozuviga (akkauntga) boshqa qurilmadan kirgan foydalanuvchi mazkur Nizomning 10-bandida belgilangan tartibda bank kartalarini biriktirishi mumkin.

3-bob. Qurilmalar va sessiyalarni boshqarish

12. Kredit va to‘lov tashkilotlari masofadan moliyaviy xizmatlarni ko‘rsatuvchi axborot tizimlari, mobil ilovalar va ularning veb-talqinidan foydalanuvchilarning qurilmalarini ro‘yxatdan o‘tkazish va monitoring qilishda quyidagi talablarga rioya etishlari shart:

mobil qurilmaning texnik identifikatsiya va dasturiy parametrlari avtomatik tarzda aniqlanishi va ma’lumotlar bazasida saqlanishini ta’minlash;

foydalanuvchining hisobga olish yozuviga (akkauntga) ro‘yxatdan o‘tmagan qurilmadan kirishga urinish holati aniqlanganda u to‘g‘risida akkaunt egasiga qurilmaning texnik parametrlarini (qurilma nomi, modeli, operatsion tizimi, IP-manzili) ko‘rsatgan holda SMS-xabarnoma orqali ogohlantirish yuborish;

SMS-xabarnomada ushbu harakatlar hisobga olish yozuvi (akkaunt) egasi tomonidan bajarilmagan bo‘lsa zudlik bilan akkauntga kirish parolini o‘zgartirish lozimligi haqida ma’lumot mavjud bo‘lishi;

yangi qurilmadan mavjud akkauntga kirishga faqatgina autentifikatsiya jarayoni yakunlanib, foydalanuvchi biometrik identifikatsiyadan o‘tganidan so‘ng ruxsat berish.

13. Foydalanuvchi mobil ilova yoki uning veb-talqinida hech qanday harakatni amalga oshirmaganda ushbu sessiyaning amal qilish vaqti 3 daqiqadan oshmasligi kerak. Bunda belgilangan vaqt tugaganidan keyin sessiya avtomatik tarzda tugatilishi va qayta autentifikatsiya talab qilinishi lozim.

14. Foydalanuvchining hisobga olish yozuviga (akkauntga) ruxsatsiz kirishga urinish yoki uning autentifikatsiya ma’lumotlari uchinchi shaxslarga oshkor bo‘lgan holatlar aniqlanganda kredit va to‘lov tashkilotlari tizimga kirish imkoniyatini to‘xtatishi va ushbu hisobga olish yozuviga (akkauntga) faqat biometrik identifikatsiyadan o‘tgan holda qayta kirishga ruxsat berishi lozim. Bunda foydalanuvchiga mazkur holat haqida SMS-xabarnoma orqali darhol xabar berilishi lozim.

Foydalanuvchining mobil qurilmasida zararli dasturlar borligi yoki masofadan boshqarilayotganligi aniqlanganda kredit va to‘lov tashkilotlari mijozga ushbu holat haqida zudlik bilan SMS-xabarnoma orqali xabar berishi lozim. SMS-xabarnomada foydalanuvchiga holatni aniqlashtirish maqsadida kredit va to‘lov tashkiloti bilan bog‘lanishi zarurligi qayd etilishi shart.

15. Kredit va to‘lov tashkilotlari mobil ilovasi o‘rnatilgan qurilmada audio/video qo‘ng‘iroqlar (shu jumladan, messenjerlar orqali audio/video qo‘ng‘iroqlar) amalga oshirilayotgan vaqtda hamda masofadan boshqarish holatida mobil ilovadan foydalanish imkoniyatini cheklashlari shart.

16. Mobil ilova va uning veb-talqinida foydalanuvchining hisobga olish yozuvi (akkaunti) doirasida “Aktiv sessiyalar” (Active Sessions) nomli alohida bo‘lim joriy etilishi va u quyidagi funksional imkoniyatlarga ega bo‘lishi lozim:

qanday qurilma(lar), brauzer(lar) va IP manzil(lar) orqali faol sessiya(lar) mavjud ekanligi to‘liq ko‘rsatilgan bo‘lishi;

har bir sessiya uchun qurilma nomi va operatsion tizim, brauzer nomi va versiyasi, IP manzili, sessiya boshlangan vaqti, joriy faol sessiya belgisi (agar ushbu sessiya foydalanuvchining hozirgi faol brauzerida ochilgan bo‘lsa) to‘g‘risidagi ma’lumotlarni o‘z ichiga olgan bo‘lishi;

har bir sessiya yonida “Sessiyani tugatish” (Log out/Terminate) tugmasi mavjud bo‘lishi va foydalanuvchi istalgan vaqtda sessiyani tugata olishi.

17. Kredit va to‘lov tashkilotlari mobil ilova orqali amalga oshiriladigan har bir moliyaviy amaliyot (bank hisobvaraqlari bo‘yicha pul o‘tkazmalari, P2P o‘tkazmalari, xizmatlar uchun to‘lovlar va boshqa operatsiyalar) foydalanuvchi tomonidan tasdiqlanishidan oldin, foydalanuvchiga ushbu amaliyot aynan mijozning o‘zi tomonidan, firibgarlar aralashuvisiz bajarilayotganligini mustaqil ravishda tasdiqlovchi ogohlantirish xabarini ko‘rsatishi shart.

Ogohlantirish xabari foydalanuvchi tomonidan tasdiqlangandan so‘ng moliyaviy amaliyotning bajarilishi davom ettirilishi lozim.

4-bob. Onlayn kredit (mikroqarz) ajratishda frod holatlarining oldini olish bo‘yicha talablar

18. Onlayn kredit (mikroqarz) olish bo‘yicha ariza kelib tushgandan so‘ng, kredit tashkiloti dastlab foydalanuvchi to‘g‘risidagi ma’lumotlarni kredit byurolari tomonidan yuritiladigan Kredit bitimini tuzish taqiqlangan shaxslar reyestridan (bundan buyon matnda reyestr deb yuritiladi) tekshirishi shart.

Foydalanuvchi to‘g‘risidagi ma’lumotlar reyestrda mavjudligi aniqlansa, onlayn kredit (mikroqarz) rasmiylashtirish jarayoni to‘xtatiladi va foydalanuvchining telefon raqamiga arizaning rad etish sababi ko‘rsatilgan holda SMS-xabarnoma yuboriladi.

Foydalanuvchi to‘g‘risidagi ma’lumotlar reyestrda mavjudligi aniqlanmasa, onlayn kredit (mikroqarz) ajratish jarayoni davom ettiriladi.

19. Kredit tashkiloti onlayn kredit (mikroqarz) ajratishda foydalanuvchining qarz yuki ko‘rsatkichi va to‘lov qobiliyatini baholash maqsadida kredit byurolariga quyidagi ma’lumotlarni o‘z ichiga olgan so‘rov yuboradi:

ariza berilgan vaqt;

arizachining rozilik bergan vaqti;

arizachining JSHSHIRi;

kreditning foiz stavkasi;

kredit muddati;

kredit summasi;

kredit turi;

valyuta turi;

kredit tarixini o‘rganish maqsadi.

20. Kredit byurolari bir JSHSHIR bo‘yicha bir vaqtning o‘zida bir nechta kredit tashkilotlaridan so‘rov kelib tushganda faqat birinchi so‘rov yuborgan kredit tashkilotining so‘roviga javob berishi shart.

Birinchi bo‘lib so‘rov yuborgan kredit tashkiloti ushbu JSHSHIR bo‘yicha onlayn kredit (mikroqarz) ajratmaslik to‘g‘risida kredit byurolariga ma’lum qilgan taqdirda kredit byurolari ushbu JSHSHIR bo‘yicha keyingi so‘rov yuborgan kredit tashkilotining so‘roviga javob berishi kerak.

Agar birinchi so‘rov yuborgan kredit tashkiloti ushbu JSHSHIR bo‘yicha onlayn kredit (mikroqarz) rasmiylashtirilganligini ma’lum qilsa, kredit byurolari mazkur JSHSHIR bo‘yicha boshqa kredit tashkilotlariga 24 soat davomida so‘rov qabul qilinmasligi to‘g‘risida ma’lumot beradi.

21. Kredit tashkiloti olingan ma’lumotlar asosida o‘zining ichki qoidalaridan kelib chiqib, onlayn kredit (mikroqarz) ajratish yoki ajratmaslik to‘g‘risida qaror qabul qiladi.

22. Kredit tashkiloti onlayn kredit (mikroqarz) ajratish to‘g‘risida qaror qabul qilsa, ariza yuborgan foydalanuvchiga uning mavjud qarzdorliklarining umumiy miqdori (agar mavjud bo‘lsa) hamda taqdim etiladigan onlayn kredit (mikroqarz)ning to‘liq qiymatini ko‘rsatgan holda mobil ilovada PUSH-xabar va telefon raqamiga SMS-xabarnoma yuborish orqali xabar beradi.

Bunda foydalanuvchiga unga yuborilgan xabardan kelib chiqib, onlayn kredit (mikroqarz) rasmiylashtirish jarayonini davom ettirish yoki bergan arizasini bekor qilish imkoniyati taqdim etilishi, shuningdek foydalanuvchi arizani bekor qilgan taqdirda unga qisqa vaqt ichida onlayn kredit (mikroqarz) olish bo‘yicha qayta ariza yuborish imkoniyati berilishi lozim.

23. Kredit tashkilotlari onlayn kredit (mikroqarz) ajratish bo‘yicha shartnoma rasmiylashtirilganidan so‘ng, pul mablag‘larini foydalanuvchiga o‘tkazib berishdan oldin foydalanuvchini masofaviy biometrik identifikatsiyadan o‘tkazishi shart.

24. Kredit tashkilotlari tomonidan onlayn kredit (mikroqarz) ajratish natijalari (onlayn kredit (mikroqarz) rasmiylashtirilgan yoki rad etilganligi to‘g‘risidagi ma’lumotlar real vaqt rejimida kredit byurolariga taqdim etilishi shart.

25. Onlayn kredit (mikroqarz) rasmiylashtirish jarayonida qarz yuki ko‘rsatkichi va kredit qobiliyatini baholash (skoring) uchun yuboriladigan so‘rovlar monitoring qilish uchun yuboriladigan so‘rovlardan alohida belgilar (identifikatorlar) bilan farq qilishi lozim.

26. Kredit tashkilotlari o‘zining ichki qoidalaridan kelib chiqib, onlayn kredit (mikroqarz) ajratish jarayonida sodir etiladigan frod holatlarining oldini olish bo‘yicha qo‘shimcha choralarni ko‘radi.

27. Kredit va to‘lov tashkilotlari o‘z mobil ilovasida foydalanuvchining hisobga olish yozuvi (akkaunti) doirasida “Firibgarlik haqida xabar berish” nomli alohida bo‘limni joriy etishi shart. Mazkur bo‘lim bosilganda alohida oyna (forma) ochilishi va unda quyidagi ma’lumotlarni kiritish uchun maydonlar taqdim etilishi lozim:

foydalanuvchining F.I.O.;

pasport yoki identifikatsiya ID-karta raqami va seriyasi;

tug‘ilgan kuni;

hisobga olish yozuvida (akkauntda) ro‘yxatdan o‘tgan telefon raqami;

firibgarlik holatining qisqacha tavsifi;

yo‘qotilgan pul mablag‘ining miqdori;

holat sodir etilgan vaqt.

5-bob. Onlayn kredit (mikroqarz) ajratishda sodir etilgan frod holatlari natijasida yetkazilgan moddiy zararni qoplash tartibi

28. Masofadan turib onlayn kredit (mikroqarz) ajratish jarayonida sodir etilgan frod holati natijasida foydalanuvchi nomiga onlayn kredit (mikroqarz) rasmiylashtirilgan taqdirda foydalanuvchi mazkur holat bo‘yicha ichki ishlar organlariga ariza bilan murojaat qiladi.

29. Ichki ishlar organlari fuqaro (foydalanuvchi) tomonidan berilgan ariza asosida sodir etilgan frod holati yuzasidan tergovga qadar tekshiruv, surishtiruv, dastlabki tergov harakatlarini

amalga oshiradi.

Tergovga qadar tekshiruv, surishtiruv, dastlabki tergov harakatlarida onlayn kredit (mikroqarz) frod holati natijasida rasmiylashtirilganligi aniqlanganda fuqaroning jabrlanuvchi deb e’tirof etilganligi to‘g‘risidagi surishtiruvchi, tergovchi, prokuror qarori yoki sudning ajrimi onlayn kredit (mikroqarz)ni rasmiylashtirgan axborot tizimi (mobil ilova, veb-talqin va boshqalar) egasi bo‘lgan kredit tashkilotiga yuboriladi.

30. Kredit tashkiloti frod holati natijasida nomiga onlayn kredit (mikroqarz) rasmiylashtirilgan fuqaroning jabrlanuvchi deb e’tirof etilganligi to‘g‘risidagi surishtiruvchi, tergovchi, prokurorning qarori yoki sudning ajrimi kelib tushgan kundan boshlab mazkur onlayn kredit (mikroqarz) va u bilan bog‘liq foizlar, neustoyka, jarimalarni hisoblashni hamda jabrlanuvchi deb e’tirof etilgan shaxsdan undirishni to‘xtatadi.

31. Kredit tashkiloti tomonidan onlayn kredit (mikroqarz) rasmiylashtirilishi va u bilan bog‘liq boshqa to‘lovlar jabrlanuvchidan undirilgan holatlarda ushbu to‘lovlar kredit tashkiloti tomonidan jabrlanuvchining bank kartasiga yoki u ko‘rsatgan hisobvarag‘iga sudning qarori yoki ajrimi asosida qaytariladi.

Mazkur to‘lovlar sudning qarori yoki ajrimi qonuniy kuchga kirgan kundan boshlab o‘n besh kun muddatda amalga oshiriladi.

32. Kredit tashkiloti onlayn kredit (mikroqarz) ajratish bilan bog‘liq frod holatini sodir etgan shaxsdan yetkazilgan moddiy zararni regress tartibida undirish maqsadida:

dastlabki tergov va sudda fuqaroviy da’vogar sifatida ishtirok etadi;

ishda ayblanuvchi tariqasida jalb etilishi lozim bo‘lgan shaxs aniqlanganda moddiy zararni undan o‘z hisobiga undirish bo‘yicha talablarni kiritadi;

qonunchilikda belgilangan tartibda boshqa harakatlarni amalga oshiradi.

33. Kredit tashkiloti frod holatiga shubha qilganda holat va dalillarni qayta tekshirish bo‘yicha tergovga qadar tekshiruv, surishtiruv, dastlabki tergov harakatlari yoki sudning qarori ustidan qonunchilikda belgilangan tartibda shikoyat qilishi mumkin.

34. Surishtiruv, dastlabki tergov natijalari yoki sudning qaroriga asosan frod holati yuz bermaganligi aniqlanganda kredit tashkiloti onlayn kredit (mikroqarz) va u bilan bog‘liq foizlar, neustoyka, jarimalarni hisoblashni hamda jabrlanuvchi deb e’tirof etilgan shaxsdan undirishni davom ettiradi.

35. Kredit tashkiloti onlayn kredit (mikroqarz) rasmiylashtirish bilan bog‘liq frod holatlari bo‘yicha kelib tushgan murojaatlar, o‘tkazilgan tekshiruv natijalari hamda qoplangan zararlar to‘g‘risidagi ma’lumotlarni har chorakda Markaziy bankka elektron shaklda taqdim etadi.

6-bob. Frod holatlarini aniqlash va oldini olish bo‘yicha talablar

36. Kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari bank kartalari, hisobvaraqlar, mobil ilovadagi hisobga olish yozuvlari (akkauntlar) hamda elektron hamyonlar bilan bog‘liq frod holatlarni aniqlash va oldini olish maqsadida session, tranzaksion antifrod va uyali aloqa darajasida axborot xavfsizligini ta’minlash tizimlarini joriy etishlari lozim.

37. Shubhali faoliyat va frod holatlarini aniqlash hamda oldini olish bo‘yicha kredit va to‘lov tashkilotlarida joriy qilingan tranzaksion antifrod tizimlari quyidagi umumiy talablarga javob berishi kerak:

foydalanuvchilarning to‘lovlarini (bank hisobvaraqlari bo‘yicha pul o‘tkazmalari, P2P o‘tkazmalar, xizmatlar uchun to‘lovlar) amalga oshirishdan oldin tahlil qilishi va frod holatlarining belgilarini aniqlashi;

frod holati belgilariga ega bo‘lgan to‘lov amaliyotlari aniqlangan taqdirda ularni to‘xtatish to‘g‘risida qaror qabul qilishi;

to‘lovni amalga oshirish bo‘yicha qaror qabul qilishdan oldin nafaqat to‘lov ma’lumotlarini balki ushbu to‘lovni amalga oshiruvchi va qabul qiluvchiga oid ma’lumotlarni (mobil ilovaning ish faoliyati jurnallari hamda session antifrod tizimlaridan olingan ma’lumotlar) tahlil qila olishi;

mobil ilova, internet-banking, avtomatlashtirilgan bank tizimi va karta protsessingi (mavjud bo‘lsa) bilan integratsiya qilish imkoniyatiga ega bo‘lishi;

foydalanuvchining harakatlarini qayd etish imkoniyatiga ega bo‘lishi;

antifrod tizimi va unda belgilangan qoidalarning samaradorligini ko‘rsatuvchi hisobotlarni sozlash imkoniyatiga ega bo‘lishi;

amaldagi axborot tizimlari va xizmatlarning uzluksiz faoliyatiga salbiy ta’sir ko‘rsatmasligi;

ma’lumotlar yaxlitligi nazorat qilingan va shifrlangan holda uzatilishi;

tashqi axborot tizimlariga (shu jumladan, tranzaksion tahlil platformalariga) qo‘shimcha tahliliy ma’lumotlarni taqdim etishi;

belgilangan ichki qoidalar asosida shubhali yoki zararli faoliyatni aniqlash va uni avtomatik bloklash imkoniyatini ta’minlashi;

proksi-server, TOR-tarmog‘i, VPN tarmog‘i va boshqa anonimlashtiruvchi vositalar orqali tizimga kirishga urinish holatlarini aniqlashi;

xosting va kolokatsiya xizmatlarini taqdim etuvchi tashkilotlarning xavf ostidagi serverlari va qurilmalaridan kirish holatlarini aniqlashi;

foydalanuvchining qurilmasiga har qanday usullardan foydalanib masofadan ruxsatsiz ulanish va boshqarish holatlarini aniqlashi.

38. Session antifrod tizimlari quyidagi talablarga javob berishi kerak:

foydalanuvchining qurilmasi va undagi xatti-harakatlari haqidagi ma’lumotlarni yig‘ish uchun mobil ilova o‘rnatiladigan iOS va Android mobil operatsion tizimlari uchun SDK (Software Development Kit), shuningdek, internet banking sahifasida joylashtiriladigan Java skriptiga ega bo‘lishi;

qurilmalar yoki SIM-kartalarning almashtirilishini aniqlashi va tahlil qilishi;

foydalanuvchi qurilmasining texnik xususiyatlari haqida ma’lumotlarni to‘plash va ular asosida qurilmaning noyob identifikatorini (qurilma barmoq izi) shakllantirishi;

mobil ilovadan foydalanish vaqtida qo‘ng‘iroqlarni (GSM/messenjerlar orqali) aniqlashi;

foydalanuvchining qurilmasini masofadan boshqarish belgilarini aniqlashi;

mobil qurilma emulyatoriga xos bo‘lgan belgilarni aniqlashi;

root/jailbreak belgilari va nosozliklarni tuzatish rejimi (debugger) yoqilganligini aniqlashi;

VPN tarmog‘idan foydalanish belgilarini aniqlashi;

sessiya ma’lumotlarini tahlil qilishi va shubhali faoliyat belgilarini aniqlashi;

tranzaksion antifrod tizimiga sessiya ma’lumotlarini yuborishi;

foydalanuvchi qurilmasini uning texnik xususiyatlari (device fingerprinting) asosida identifikatsiya qilishi;

foydalanuvchi qurilmasini global (cross-client) darajasida identifikatsiya qilishi;

foydalanuvchining hisobga olish yozuvi (akkaunti)dan ruxsatsiz foydalanish holatlarini aniqlashi;

himoyalangan veb-ilovaga uchinchi tomon kodi kiritilgan (ineksiya) holatlarni aniqlashi;

server tomondagi veb qismga frod yo‘li bilan kiritilgan (veb-ineksiya) kodlarni aniqlashi;

fishing holatlarini aniqlashi;

xavf darajasini baholash maqsadida har bir foydalanuvchi ishlatayotgan brauzerlarni monitoring qilishi;

qurilma identifikatorlarini o‘zgartirish yoki yashirish imkonini beruvchi maxsus brauzerlar (antidetect) orqali kirish holatlarini aniqlashi;

foydalanuvchi xatti-harakatlari (navigatsiya, kursor harakati, tugmalarni bosish tezligi, tanaffuslar va forma bilan o‘zaro ta’sir) asosida asl foydalanuvchi va firibgarlik faoliyatini farqlash mexanizmlarini joriy etishi;

avtomatik kirishga urinishlar (bruteforce) va boshqa manbalardan olingan buzilgan autentifikatsiya ma’lumotlarini qo‘llab (credential stuffing) tizimga kirishga urinish holatlarini aniqlashi va bloklashi;

tashqi tizimlarga kirishga urinish holatlari bo‘yicha ma’lumot taqdim etishi;

mobil ilovadan foydalanish vaqtida foydalanuvchining harakatlari haqida ma’lumot yuborishi;

brauzerlardan ma’lumot olishi (shuningdek, Chromium 26, Microsoft Edge 13, Mozilla Firefox 4, Safari 8 va undan past bo‘lgan versiyalar ishlatilganda bloklashi);

foydalanuvchi tomonidan bir nechta qurilma yoki SIM-karta almashinuvini aniqlashi va tahlil qilishi;

mobil ilovadagi xatti-harakatlar (teginishlar, surishlar, matn terish tezligi, sensor ma’lumotlari) asosida foydalanuvchi yoki firibgar faoliyatini aniqlashi;

GPS va Wi-Fi tarmog‘i ma’lumotlari orqali joylashuvga oid shubhali faoliyatni aniqlashi;

foydalanuvchi va dasturiy ta’minotning zararli faoliyatini tashkilot tomonidan tanlangan qoidalar asosida bloklashi;

foydalanuvchi sessiyasida mobil ilovaning nosozliklarini topish vositasi (debugger) yoqilgan holatlarni aniqlashi va foydalanuvchi harakatlarini tahlil qilishda inobatga olishi;

mobil ilova va server (yoki boshqa xizmatlar) o‘rtasida ma’lumot almashish uchun mo‘ljallangan dasturiy interfeys (Application Programming Interface)ni botlar yoki tashqi tizimlar foydalanishidan himoyalashi.

39. Kredit va to‘lov tashkilotlari shubhali va bloklangan operatsiyalar yuzasidan quyidagi ma’lumotlarni to‘plab, elektron tarzda hujjatlashtirishi lozim:

operatsiya sanasi va vaqti;

foydalanuvchining identifikatori va qurilma ma’lumotlari;

operatsiya turi va miqdori;

xavfni aniqlash sabablari;

ko‘rilgan choralar (bloklash, xabar yuborish, aloqaga chiqish, tahlil qilish va h.k.);

yakuniy qaror.

Ushbu ma’lumotlar kredit tashkilotlarida kamida 3 yil davomida saqlanishi shart.

40. Mobil ilovalar yoki veb-resurslar orqali bank kartasining SMS-xabarnoma xizmatini yoqish, o‘chirish yoki o‘zgartirish taqiqlanadi.

41. Mobil ilovada bank kartasi egasining ismi to‘liq shaklda, familiyasining esa faqat birinchi harfi aks ettirilishi, pul o‘tkazmalari amalga oshirilganda mazkur telefon raqamga ulangan bank kartalari egasining ma’lumotlari qisman berkitilgan tarzda aks ettirilishi lozim.

42. Tashqi tizimlar yoki xorijiy tashkilotlarning mobil ilovalaridan xalqaro o‘tkazmalar telefon raqami orqali amalga oshirilganda bank kartasi egasining ismi to‘liq shaklda,

familiyasining birinchi harfi aks ettirilishi hamda bank kartasining birinchi va oxirgi to‘rtta raqamlari jo‘natuvchi interfeysida aks ettirilishi lozim.

43. Kredit tashkilotida onlayn kredit (mikroqarz) ajratish va omonat operatsiyalarini real vaqt rejimida kuzatib borish imkonini beradigan tranzaksion monitoring tizimi joriy etilishi lozim.

Elektron hamyonlar bilan ishlovchi kredit va to‘lov tashkilotlarida shubhali tranzaksiyalarni aniqlash va oldini olish bo‘yicha tranzaksion antifrod tizimi joriy etilishi lozim.

44. Kredit tashkilotlari axborot xavfsizligi va kiberxavfsizlikni ta’minlash va frod holatlariga tezkor javob qaytarish maqsadida foydalanuvchilarni quyidagi holatlar yuz berganda SMS-xabarnoma va mobil ilovada PUSH-xabar orqali zudlik bilan xabardor qilishi hamda jarayonni to‘xtatishi va foydalanuvchining qo‘shimcha tasdiqdan o‘tishini ta’minlashi shart:

foydalanuvchi nomidan yangi qurilma orqali tizimga kirishga urinishda;

foydalanuvchi nomidan onlayn kredit (mikroqarz) rasmiylashtirish, omonat joylashtirish hamda omonatdan pul mablag‘larini yechib olish bo‘yicha so‘rov yuborilganda;

tizimda frod alomatlari qayd etilganda (qisqa vaqt ichida bir nechta operatsiyalarning amalga oshirilishi, shubhali IP-manzillardan kirish, noodatiy geolokatsiyadan harakatlar va boshqalar).

45. Masofadan moliyaviy xizmatlarni taqdim etuvchi axborot tizimlari, shuningdek, mobil ilovalarga nisbatan amalga oshiriladigan kibertahdidlar maxsus platformalar orqali monitoring va tahlil (threat intelligence) qilish jarayonida aniqlangan vaqtda tizim orqali zudlik bilan Markaziy bankka xabar berilishi lozim.

7-bob. Ma’lumotlarni saqlash va muhofaza qilish

46. Kredit va to‘lov tashkilotlari jismoniy shaxslarning shaxsiga doir, identifikatsiya va to‘lov bilan bog‘liq barcha turdagi ma’lumotlarning xavfsizligini ta’minlash maqsadida ularni o‘z axborot tizimlarida shifrlangan holda saqlashi shart.

Axborot tizimlaridagi ma’lumotlarning ruxsatsiz tarqalishining oldini olish maqsadida ma’lumotlarni ruxsatsiz tarqalishidan himoyalash tizimi DLP (Data Loss Prevention) joriy etilishi lozim.

47. Axborot tizimida foydalanuvchi va tizimning o‘zi tomonidan amalga oshirilgan barcha harakatlar avtomatik tarzda jurnallashtirilishi shart. Jurnallar soxtalashtirish va o‘zgartirishdan himoyalangan formatda saqlanishi lozim. Jurnal ma’lumotlarining yaxlitligini ta’minlash maqsadida WORM (Write Once Read Many) texnologiyasidan foydalanish tavsiya etiladi.

48. Imtiyozli funksiyalar va yuqori darajadagi tizim huquqlari orqali amalga oshirilgan barcha harakatlarga faqat cheklangan doiradagi xodimlar tomonidan kirishga ruxsat berilishi shart. Bunday huquqlardan foydalanish jarayonlari majburiy tarzda ko‘p omilli autentifikatsiya MFA (Multi-Factor Authentication) orqali himoyalanishi lozim.

Imtiyozli funksiyalar va yuqori darajadagi tizim huquqlari doirasida amalga oshiriladigan faoliyatning to‘liq nazorati va jurnallashtirilishi PAM (Privileged Access Management) tizimi orqali amalga oshirilishi kerak.

49. Kredit va to‘lov tashkilotlari axborot tizimlaridagi ma’lumotlarni himoya qilish uchun kriptografik himoya vositalaridan foydalanishda quyidagi talablarni bajarishlari shart:

aloqa kanallari orqali axborot almashinuvini faqat himoyalangan Transport Layer Security (TLS) protokolidan (1.3 yoki undan yuqori versiya) foydalangan holda amalga oshirish;

ma’lumotlarni shifrlashda AES-256/GCM algoritmidan foydalanish;

kriptografik kalitlarning aylanish (rotatsiya) siyosatini kiberxavfsizlik sohasidagi vakolatli davlat organi tomonidan belgilangan talablar doirasida amalga oshirish;

kriptografik kalitlar kamida yilda bir marotaba yangilanib borilishini ta’minlash;

kriptografik kalitlar bilan bog‘liq barcha yozuvlar (loglar), shu jumladan kalit yaratish, aylantirish, bekor qilish va foydalanish holatlari to‘g‘risidagi ma’lumotlarni kamida 3 yil davomida saqlash;

kriptografik kalitlarning muddati o‘tganidan keyin ularni belgilangan tartibda yo‘q qilish yoki arxiv holatiga o‘tkazish hamda bu jarayonni tegishli dalolatnoma bilan rasmiylashtirish.

50. Kredit va to‘lov tashkilotlari kriptografik kalitlarni boshqarishda kalitlarni boshqarish tizimi (KMS) yoki apparat xavfsizlik moduli (HSM)dan foydalanishlari mumkin.

51. Mazkur Nizomda qayd etilgan kriptografik algoritmlar yoki protokollarning versiyalari (jumladan, TLS, AES va boshqalar) eskirgan yoki zaif deb topilsa, kredit va to‘lov

tashkilotlari ma’lumotlarni himoya qilishda yangilangan, ekvivalent yoki undan yuqori darajadagi xavfsizlikni ta’minlaydigan kriptografik algoritmlar va protokollardan foydalanishlari lozim.

52. Kredit va to‘lov tashkilotlari axborot tizimlari doirasida amalga oshirilgan barcha texnik jarayonlar, foydalanuvchi faoliyati, xavfsizlik bilan bog‘liq holatlar, operatsiya jurnallari va tegishli dasturiy yozuvlarni kamida 3 yil mobaynida xavfsiz va ishonchli shaklda saqlashi lozim.

8-bob. Mobil ilovalar va ularning veb-talqinida xavfsizlikni ta’minlash

53. Kredit va to‘lov tashkilotlari tomonidan joriy etilgan mobil ilovalar va ularning veb-talqini axborot xavfsizligi va kiberxavfsizlikni ta’minlash talablariga to‘liq javob berishi lozim.

54. Mobil ilovaga texnik xavf tug‘diruvchi qurilmalarda ishlashini avtomatik tarzda aniqlash va bloklash mexanizmlari joriy etilishi lozim.

55. Kredit va to‘lov tashkilotlari quyidagi holatlarda mobil ilovaning ishlashini cheklashi lozim:

android operatsion tizimida ishlovchi qurilmaning tizim huquqlariga noqonuniy kirish orqali xavfsizlik siyosati buzilganda (root);

iOS operatsion tizimida ishlovchi qurilmada ishlab chiqaruvchi tomonidan o‘rnatilgan xavfsizlik cheklovlari o‘chirilib, tizimga chuqur kirish imkoniyati yaratilganda (jailbreak).

56. Mobil ilova ishga tushirilganda qurilmaning xavfsizlik holati tahlil qilinishi (SafetyNet Attestation, Play Integrity API, Jailbreak detection kabi vositalar) va salbiy holat aniqlanganda mobil ilovaning ish faoliyati to‘xtatilib, foydalanuvchiga SMS-xabarnoma yuborilishi shart. Ushbu holat bayonnoma (loglar) bazasiga avtomatik tarzda qayd etilishi lozim.

57. Mobil ilova dastur kodiga ruxsatsiz kirish, tahrirlash, teskari muhandislik (reverse engineering) va dekompilyatsiya orqali tahlil qilish imkoniyatini cheklovchi maxsus texnologiyalar bilan himoya qilinishi shart.

58. Kredit va to‘lov tashkilotlari mobil ilova orqali tarqalishi mumkin bo‘lgan zararli kodlar, dasturlar va frodga oid tahdidlarni aniqlash va ularning oldini olish maqsadida mobil SDK (Software Development Kit) orqali antivirus va antifrod funksiyalari bilan ta’minlangan xavfsizlik modullarini integratsiya qilishi kerak.

59. Kredit va to‘lov tashkilotlari mobil ilovani real vaqt rejimida tahdidlardan himoya qilish uchun RASP (Runtime Application Self-Protection) texnologiyalarini joriy qilishi lozim.

60. Kredit va to‘lov tashkilotlari o‘z veb-talqinlarida quyidagi axborot xavfsizligi va kiberxavfsizlikni ta’minlash choralarini ko‘rishlari shart:

ma’lumot almashinuvi HTTPS protokoli orqali amalga oshirilishi va HSTS (Strict Transport Security) siyosati faollashtirilishi;

veb-talqinga yuklanadigan JavaScript kodlarining yaxlitligini ta’minlash uchun SRI (Subresource Integrity) yoki shunga mos mexanizmlar qo‘llanishi;

brauzer muhitida anomal faollikni (bot faolligi, avtokliker, virtual muhit) aniqlash uchun tegishli kiberxavfsizlik vositalarini joriy qilishi.

61. Kredit va to‘lov tashkilotlari mobil ilovalar va ularning veb-talqinida sessiya boshqaruvi hamda autentifikatsiya xavfsizligini o‘zining antifrod tizimlarida belgilangan talab va qoidalarga asosan ta’minlaydi.

62. Foydalanuvchining faoliyati, sessiyalari, anomal harakat va tahdidlar bilan bog‘liq barcha ma’lumotlar bayonnomalashtirilishi (loglash) hamda markazlashgan monitoring (SIEM) tizimiga integratsiya qilingan holda real vaqt rejimida kuzatilishi va qayd etilishi shart.

63. Kredit va to‘lov tashkilotlarining mobil ilovalariga qisqa vaqt oralig‘ida noodatiy darajada ko‘p so‘rovlar kelib tushganda axborot tizimining barqarorligi va xavfsizligini ta’minlash maqsadida bunday so‘rovlarga nisbatan cheklovlar joriy etishi, vaqtinchalik bloklash yoki boshqa himoya choralarini mustaqil ravishda qo‘llashlari lozim.

64. Mobil ilovadagi akkauntga 1 daqiqa mobaynida 1 ta IP manzildan 2 va undan ortiq qurilmadan urinish holatlari kuzatilsa, ushbu akkaunt 10 daqiqaga bloklanishi lozim.

9-bob. Foydalanuvchilarni o‘qitish va ma’lumot berish

65. Kredit va to‘lov tashkilotlari o‘z axborot tizimlari, mobil ilovalari va veb-resurslarida ro‘yxatdan o‘tgan foydalanuvchilarini axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda frod holatlarining oldini olish bo‘yicha asosiy qoidalar bilan tanishtirishi shart.

66. Axborot tizimlari, mobil ilovalar va veb-resurslarda foydalanuvchiga frodning turlari, eng ko‘p uchraydigan sxema va usullari hamda ulardan himoyalanish bo‘yicha amaliy tavsiyalar berib borilishi lozim.

67. Kredit tashkilotlari frod holatlari to‘g‘risida foydalanuvchilar tezkor murojaat qilishlari uchun bank kartasining orqa tomonida 24/7 rejimda ishlovchi aloqa raqamini ko‘rinib turadigan va o‘qish uchun oson shaklda joylashtirishi shart.

68. Kredit va to‘lov tashkilotlari bank kartasini rasmiylashtirish yoki boshqa turdagi xizmatlarni taqdim etish jarayonida tuziladigan shartnomalar va ommaviy ofertalarda quyidagi talablarni belgilashi shart:

foydalanuvchiga kredit va to‘lov tashkilotlari tomonidan yuboriladigan xabarlar, jumladan mobil ilovadagi bildirishnomalar, SMS va PUSH-xabarlarni diqqat bilan o‘rganib chiqishi shartligi;

kredit va to‘lov tashkilotlari tomonidan foydalanuvchiga firibgarlik belgilari aniqlanganligi to‘g‘risida ma’lumot berilishi;

foydalanuvchi kredit yoki to‘lov tashkilotidan shu kabi xabarlarni olganidan keyin har qanday to‘lov amaliyotlarini tasdiqlashda ehtiyotkor bo‘lishi;

foydalanuvchining qurilmasi yo‘qolganligi yoki uchinchi shaxslar tomonidan qurilmani boshqarishga nazorat o‘rnatilganligini aniqlagan paytdan boshlab zudlik bilan biroq 1 kundan kechiktirmay kredit yoki to‘lov tashkilotini xabardor qilishi;

foydalanuvchi o‘z roziligisiz amalga oshirilgan operatsiya faktini aniqlagan paytdan boshlab 1 kun ichida bu haqda kredit va to‘lov tashkilotini xabardor qilishi;

foydalanuvchi kredit va to‘lov tashkilotiga o‘zining aloqa ma’lumotlarini taqdim etishi shartligi, ushbu ma’lumotlar kredit va to‘lov tashkilotining foydalanuvchi bilan bog‘lanishi uchun zarurligi, agar ushbu ma’lumotlar o‘zgarsa, foydalanuvchi o‘zgarishlar sodir bo‘lgan kundan boshlab 3 kun ichida bu haqda kredit yoki to‘lov tashkilotiga xabar berishi.

Kredit va to‘lov tashkilotining so‘roviga ko‘ra foydalanuvchi operatsiyani o‘zi mustaqil ravishda amalga oshirganligi yoki uni foydalanuvchining topshirig‘i yoxud ixtiyoriy roziligi bilan uchinchi shaxs bajarganligi haqidagi ma’lumotlarni taqdim etishi shart. Shuningdek, foydalanuvchi firibgarlik holatlari to‘g‘risidagi ma’lumotlarni ham taqdim etishi lozim.

69. Bank kartasini rasmiylashtirish jarayonida foydalanuvchilarga bank kartasining amal qilish muddati, himoya parollari va telefon raqamiga SMS orqali yuboriladigan bir martalik tasdiqlovchi kodlarni begona shaxslarga taqdim etmaslik to‘g‘risida tushuntirish hamda yozma ravishda ma’lumot berilishi lozim.

70. Foydalanuvchi SMS-xabarnoma xizmatiga ulangan telefon raqamini o‘zgartirgan taqdirda kredit va to‘lov tashkiloti uning avvalgi telefon raqamiga xizmatning o‘chirilganligi va

yangi telefon raqamiga xizmatning ulanganligi haqida SMS-xabarnoma orqali xabar berishi shart.

10-bob. Yakuniy qoidalar

71. Mazkur Nizom talablarining buzilishida aybdor bo‘lgan shaxslar qonunchilik hujjatlarida belgilangan tartibda javobgar bo‘ladilar.

72. Mazkur Nizomning 5-bobida belgilangan talablar Nizom kuchga kirgandan keyin sodir etilgan onlayn kredit (mikroqarz) ajratish bilan bog‘liq frod holatlariga nisbatan qo‘llaniladi.

73. Mazkur Nizomda belgilangan talablarning agent va subagentlar tomonidan bajarilishi ularga tegishli asosiy tashkilot (kredit yoki to‘lov tashkiloti) tomonidan nazorat qilinadi.