O‘ZBEKISTON RESPUBLIKASI
ADLIYA VAZIRLIGIDA
DAVLAT RO‘YXATIDAN O‘TKAZILDI
RO‘YXAT RAQAMI: 3513
2024 - yil 21 - may

O'ZBEKISTON RESPUBLIKASI MARKAZIY BANKI BOSHQARUVINING QARORI

To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarni oldini olish choralarini ko‘rish to‘g‘risidagi nizomni tasdiqlash haqida

O‘zbekiston Respublikasining “O‘zbekiston Respublikasining Markaziy banki to‘g‘risida”gi va “Kiberxavfsizlik to‘g‘risida”gi qonunlari, O‘zbekiston Respublikasi Prezidentining 2023-yil 30-noyabrdagi PQ–381-son “Raqamli mahsulotlar (xizmatlar) iste’molchilari huquqlarini himoya qilish va raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarga qarshi kurashishni kuchaytirish choralari to‘g‘risida”gi qaroriga muvofiq O‘zbekiston Respublikasi Markaziy banki boshqaruvi **qaror qiladi:**

1. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarni oldini olish choralarini ko‘rish to‘g‘risidagi nizom ilovaga muvofiq tasdiqlansin.

2. O‘zbekiston Respublikasi Markaziy banki boshqaruvining 2020-yil 11-iyundagi 13/10-son “To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarining to‘lov tizimlarida axborot xavfsizligini ta’minlash to‘g‘risidagi nizomni tasdiqlash haqida”gi qarori (ro‘yxat raqami 3268, 2020-yil 30-iyun) (Qonun hujjatlari ma’lumotlari milliy bazasi, 30.06.2020-y, 10/20/3268/1112-son) o‘z kuchini yo‘qotgan deb topilsin.

3. Mazkur qaror O‘zbekiston Respublikasi Davlat xavfsizlik xizmati, Raqamli texnologiyalar vazirligi, Ichki ishlar vazirligi, Istiqbolli loyihalar milliy agentligi hamda Elektron texnologiyalarini rivojlantirish markazi bilan kelishilgan.

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

Марказий банк раиси **Nurmuratov M. B.**

Тошкент ш.
2024 йил 24 апрель,
13/1 сон

Келишилди:

Ўзбекистон Республикаси ДХХ Раиси

Azizov A. A.

Тошкент ш.
2024 йил 19 апрель,

Ўзбекистон Республикаси Электрон технологияларини ривожлантириш маркази бошлиғи

Xodjakbarov O. T.

Тошкент ш.
2024 йил 23 апрель,

Лойиҳа бошқаруви миллий агентлиги Директори

Li D. R.

Тошкент ш.
2024 йил 23 апрель,

Ўзбекистон Республикаси Ички ишлар вазири

Бобожонов П.Р.

Тошкент ш.
2024 йил 01 апрель,

O‘zbekiston Respublikasi Raqamli texnologiyalar vaziri

Shermatov Sh. X.

Тошкент ш.
2024 йил 29 март,

O‘zbekiston Respublikasi
Markaziy banki boshqaruvining
2024-yil 24-apreldagi
13/1-son qaroriga
ILOVA

To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarni oldini olish choralarini ko‘rish to‘g‘risidagi
NIZOM

Mazkur Nizom to‘lov tizimi operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarni oldini olishga doir talablarni belgilaydi.

1-bob. Umumiy qoidalar

1. Mazkur Nizomda quyidagi asosiy tushunchalardan foydalaniladi:

avtorizatsiya – ma’lum shaxsga yoki shaxslar guruhiga muayyan harakatlarni amalga oshirish huquqini berish;

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

identifikatsiya – to‘lov tizimlari subyektlariga identifikator tayinlash va/yoki belgilangan identifikatorlar ro‘yxati bilan identifikatorlarni taqqoslash;

kriptografik kalit – elektron raqamli imzoni hisoblash yoki tekshirish, shuningdek shifrlash va dastlabki matnga o‘girish uchun qo‘llaniladigan simvollar ketma-ketligi;

masofaviy xizmat ko‘rsatish tizimi – elektron xizmatlardan foydalanish uchun to‘lov xizmatlaridan foydalanuvchi va ushbu xizmatlarni yetkazib beruvchi o‘rtasidagi aloqani ta’minlaydigan telekommunikatsiya vositalari, raqamli va axborot texnologiyalari, dasturiy ta’minot va uskunalar majmui;

muhim to‘lov tizimlari operatorlari – to‘lov tizimining ishidagi to‘xtalishlar (uzilishlar) O‘zbekiston Respublikasi to‘lov xizmatlari bozorida tavakkalchiliklarning paydo bo‘lishiga olib kelishi mumkin bo‘lgan hamda O‘zbekiston Respublikasi Markaziy banki (bundan buyon matnda Markaziy bank deb yuritiladi) tomonidan muhim to‘lov tizimi jumlasiga kiritilgan to‘lov tizimining operatori hisoblangan yuridik shaxs;

to‘lov – pul majburiyatini naqd pul mablag‘lari bilan bajarish yoxud pul mablag‘larini to‘lov vositalaridan foydalangan holda o‘tkazish;

to‘lov agenti – bank yoki to‘lov tashkiloti bilan to‘lov xizmatlari ko‘rsatish uchun agentlik shartnomasini tuzgan, bank hisoblanmaydigan yuridik shaxs;

to‘lov subagenti – to‘lov agenti bilan to‘lov xizmatlarini ko‘rsatish bo‘yicha subagentlik shartnomasini tuzgan, bank hisoblanmaydigan yuridik shaxs yoki yakka tartibdagi tadbirkor;

to‘lov tashkiloti – bank hisoblanmaydigan, to‘lov xizmatlarini ko‘rsatish bo‘yicha faoliyatni amalga oshirishga vakolatli bo‘lgan yuridik shaxs;

to‘lov tizimlari operatorlari – O‘zbekiston Respublikasi hududida to‘lov tizimining ishlashini ta’minlash bo‘yicha faoliyatni amalga oshiruvchi yuridik shaxs;

to‘lov tizimining ishtirokchilari – to‘lov tizimi operatori bilan hisob-kitoblarni amalga oshiruvchi va to‘lov tizimlarida ishtirok etish to‘g‘risida shartnoma tuzgan banklar;

to‘lov xizmatlarini yetkazib beruvchilar – O‘zbekiston Respublikasi Markaziy banki, banklar, to‘lov tashkilotlari, to‘lov agentlari, to‘lov subagentlari;

kliring – to‘lov tizimi ishtirokchilarining pulga doir o‘zaro talablari va majburiyatlarini yig‘ish, taqqoslash hamda hisobga o‘tkazish jarayoni;

elektron pullar – elektron pullar emitentining elektron shaklda saqlanadigan hamda elektron pullar tizimida to‘lov vositasi sifatida qabul qilinadigan shartsiz va chaqirib olinmaydigan pul majburiyatlari;

axborotlashtirish obyekti – turli darajadagi va maqsadlardagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotga ishlov berishning texnik vositalari, ushbu vositalar o‘rnatilgan va ishlatiladigan xonalar, shuningdek muzokaralar, shu jumladan maxfiy muzokaralar olib borish uchun mo‘ljallangan alohida xonalar;

antifrod tizimi – bank kartalari va hisobvaraqlari, mobil ilovalar akkauntlari hamda elektron hamyonlar yordamida to‘lovlarni amalga oshirishda sodir etiladigan firibgarlikni oldini olishga qaratilgan jarayonlar yig‘indisi;

frod – axborot texnologiyalarini qo‘llagan holda sodir etiladigan firibgarlik harakatlari;

axborot xavfsizligi – axborot munosabatlarining subyektlariga nomaqbul ziyonlarni keltirishi mumkin bo‘lgan tabiiy yoki sun’iy xususiyatli tasodifiy yoki qasddan qilingan ta’sirlardan axborot va ta’minlab turadigan infratuzilmaning muhofaza qilinganligi;

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

xavfsizlik rejimi – normativ-huquqiy hujjatlar va texnik jihatdan tartibga solish sohasidagi normativ hujjatlar bilan belgilangan, ma’muriy-huquqiy, tashkiliy, injener-texnik va boshqa chora-tadbirlarni o‘z ichiga oladigan, tashkilotning konfidensial ma’lumotlaridan noqonuniy foydalanishning oldini olishni ta’minlovchi tartib.

2-bob. To‘lovlar to‘g‘risidagi axborotni himoya qilish

2. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar o‘zlarining axborot tizimlari xususiyatlaridan kelib chiqib, axborot xavfsizligi siyosatini ishlab chiqadi.

3. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar to‘lovlar to‘g‘risidagi axborotni shakllantirish, uzatish, saqlash va unga ishlov berishning barcha bosqichlarida to‘lovlar to‘g‘risidagi axborotni uzluksiz himoya qilish uchun quyidagi choralarni ko‘rishlari lozim:

identifikatsiya, autentifikatsiya va avtorizatsiya qilish tizimini joriy etish;

tizimga ruxsatsiz kirishning oldini olish usullarini (login, parol, biometrik identifikatsiya, ikki faktorli autentifikatsiya (2FA) va boshqa) qo‘llash;

to‘lov hujjati va identifikatsiya ma’lumotlarini qalbakilashtirish, ularni ruxsatsiz o‘zgartirish hamda uchinchi shaxslarga taqdim etishdan himoyalash;

to‘lov axborotlari shakllantirilishini, to‘lov hujjatining haqqoniyligi tekshirilishini va ularga ishlov berilishini hamda asosli o‘zgartirishlar kiritilishini ta’minlash va nazorat qilish;

to‘lov hujjatlarini uzatishda ushbu hujjatning asl egasiga yetkazilishini hamda boshqa shaxslarga jo‘natilishining oldi olinishini ta’minlash;

amalga oshirilgan to‘lovga oid ma’lumotlarni saqlashda ularni ruxsatsiz ko‘chirish, o‘zgartirish, o‘chirish hamda uchinchi shaxslarga jo‘natilishining oldini olish choralarini ko‘rish;

tashqi saqlovchiga ko‘chirilgan to‘lovga oid ma’lumotlarning seyfda (temir shkafda) saqlanishini ta’minlash hamda ma’lumotlarni saqlash uchun mas’ul xodim (xodimlar) tayinlash;

axborot tizimlaridagi dasturiy ta’minotlarning nazoratini va hisobini yuritish hamda axborot tizimlaridagi dasturiy ta’minot talqinlarining, apparat-dasturiy qurilmalarining va dasturiy vositalarining uzluksiz ishlashini ta’minlash;

axborot tizimlarining aktual holatda (oxirgi versiya) bo‘lishini ta’minlash, bunda dasturiy ta’minotning yangi talqinini tekshiruvdan o‘tkazgandan so‘ng axborot tizimiga joriy etish;

to‘lov axborotlariga ishlov berish, ularni uzatish hamda saqlash jarayonlarini elektron bayonnomalarda avtomatik tarzda shakllantirib borish hamda ularning saqlanishini ta’minlash;

axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati hamda bank va to‘lov tizimlarida shubhali frod operatsiyalarga qarshi choralar ko‘rish xizmatlarini tashkil etish, shuningdek axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda bank kartalari bilan bog‘liq shubhali (frod) operatsiyalarga qarshi choralar ko‘rish bo‘yicha amalga oshiriladigan ishlarni nazorat qilish;

hisoblash tarmog‘ining xavfsizligi va kriptografik muhofazasini ta’minlash, kompyuter viruslaridan himoyalash, axborot tizimlariga kirishni boshqarish, texnik vositalarini sozlash va boshqa choralarni qo‘llash;

axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda bank kartalari bilan bog‘liq shubhali (frod) operatsiyalarga qarshi choralar ko‘rish uskunalari, qurilmalar, apparat-dasturiy va dasturiy texnik vositalari qo‘llanishini ta’minlash hamda ularni muntazam takomillashtirib borish, foydalanish tartiblarini belgilash, ularga texnik xizmat ko‘rsatish, ta’mirlash va boshqa holatlarda ulardan ko‘zda tutilmagan tarzda ruxsatsiz foydalanishning oldini olish;

qo‘llanilayotgan texnik vositalarga barcha telekommunikatsiya tarmoqlaridan ruxsatsiz kirish, ulardagi ma’lumotlarni o‘zgartirish, o‘chirish, ko‘chirib olishdan himoyalash;

axborotlarni chiqib ketishi (yo‘qolishini) oldini olish;

axborot tizimiga ruxsatsiz kirish yoki kiberxavfsizlik hodisalari sodir etilganda, ularni tahlil qilish asosida himoya tizimlarini mustahkamlab borish choralarini ko‘rish.

4. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar dasturlarga va operatsion tizimga zarar keltiruvchi zararli kodlar (kompyuter viruslari) va ularning salbiy ta’sirining oldini olish uchun quyidagi choralarni ko‘rishi kerak:

hisoblash texnikasi qurilmalari (serverlar, kompyuterlar va boshqalar), bankomat, embosser va to‘lov terminallarining (texnik imkoniyatidan kelib chiqib) ish faoliyatiga zarar yetkazuvchi kodlarni (kompyuter viruslarini) aniqlash va ularning salbiy ta’sirining oldini olish choralarini ko‘rish;

axborot tizimlarida faqat litsenziyalangan antivirus dasturidan foydalanish, ularning rusumlari va

bazalari aktualligi hamda yangilanib borilishini ta’minlash;

antivirus dasturlarining avtomatik tarzda ishlashini ta’minlash;

internet va korporativ tarmoqlar orqali kelgan barcha axborotlarni antivirus dasturi orqali tekshirish.

5. To‘lov tizimlarida axborotni muhofaza qilishning kriptografik usullari qo‘llanilishi va to‘lov tizimi qoidalarida quyidagilar belgilab berilishi lozim:

kriptografik muhofaza vositalarini avtomatlashtirilgan tizimlarga bog‘lash, ishga tushirish, ishlatish va foydalanishdan chiqarish tartibi;

kriptografik muhofaza vositalarining to‘xtab qolishi, ishdan chiqishi va boshqa favqulodda holatlarda ularni qayta tiklash tartibi;

kriptografik muhofaza dasturlariga va texnik hujjatlariga o‘zgartirishlar kiritish tartibi;

kriptografik kalitlarni boshqarish tartibi;

kriptografik kalitlarni tashuvchi qurilmalarni qo‘llash, saqlash, o‘zgartirish va boshqalar bo‘yicha tashkiliy, texnikaviy usullarni qo‘llash tartibi.

To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar O‘zbekiston Respublikasi Markaziy banki bilan axborot almashinuvida axborot xavfsizligi hamda kiberxavfsizlikni ta’minlashlari shart.

6. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning axborotlashtirish obyektlariga ruxsatsiz kirish hamda foydalanishni chegaralash maqsadida quyidagi choralar ko‘rilishi kerak:

axborotlashtirish obyektlariga, shu jumladan, bankomat, to‘lov terminallari va to‘lov o‘tkazish elektron qurilmalariga jismonan ta’sir etishni hamda texnik jihozlar mavjud bo‘lgan bino va xonalarga kirishni nazorat qilish;

to‘lovlarni amalga oshirishda qo‘llaniladigan avtomatlashtirilgan tizimlar, dasturlar, hisoblash texnikalari, telekommunikatsiya qurilmalari parametrlari va tuzilmalari hamda to‘lov tizimida ishlash huquqini beruvchi ma’lumotlarni (parol, biometrik va boshqa ma’lumotlar) o‘z ichiga olgan texnik vositalarning jismoniy muhofazasini (xavfsizlik rejimini) ta’minlash va ruxsatsiz ta’sir etishning oldini olish;

to‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning xodimlari axborotlashtirish obyektlariga kirishini nazorat qilish va ma’lumotlarni ruxsatsiz tarqalishidan himoyalash tizimlarini joriy qilish;

serverlar va telekommunikatsiya qurilmalari joylashgan xonalarda ishlash jarayonlarini videokuzatuv tizimlari yordamida nazorat qilish.

7. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar quyidagi ma’lumotlarni o‘z ichiga olgan axborot tizimlarining axborot xavfsizligi va kiberxavfsizligini ta’minlashlari kerak:

bank (karta) hisobvarag‘ida pul mablag‘lari qoldiqlari to‘g‘risidagi ma’lumotlar;

elektron pullar qoldiqlari to‘g‘risidagi ma’lumotlar;

amalga oshirilgan to‘lovlar to‘g‘risidagi ma’lumotlar;

naqd pulsiz hisob-kitoblarni o‘z ichiga olgan ma’lumotlar;

banklararo to‘lov va kliring tizimlari to‘lov ma’lumotlari;

kriptografik muhofazani ta’minlash uchun qo‘llaniladigan kriptografik kalitlar;

to‘lovlarni amalga oshirishda qayta ishlanadigan konfidensial axborotlarni (bank siri, shaxsga doir ma’lumotlar va boshqa qonun bilan muhofaza qilinadigan ma’lumotlar);

mijozlarning bank kartalari, akkauntlari va identifikatsiyadan o‘tganligi to‘g‘risidagi ma’lumotlar.

8. To‘lov tizimlari operatorlari yoki to‘lov xizmatlarini yetkazib beruvchilar masofadan to‘lov xizmatlarini ko‘rsatuvchi axborot tizimlarini (mobil ilova, internet banking va boshqalar) (bundan buyon matnda masofaviy axborot tizimlari deb yuritiladi) amaliyotga joriy etish hamda ularga o‘zgartirish kiritishdan avval quyidagilarni ta’minlashlari lozim:

masofaviy axborot tizimlarining to‘lovlarni o‘tkazish bilan bog‘liq barcha funksiyalarini sinov (test) tarzida to‘liq tekshiruvdan o‘tkazishni ta’minlash;

masofaviy axborot tizimlarini texnik topshiriqlar, ularni texnik topshiriqqa va kiberxavfsizlik talablariga muvofiqligi yuzasidan ekspertizadan o‘tkazish hamda ularning natijalari bo‘yicha ekspertiza xulosalarini Markaziy bankka taqdim etish;

masofaviy axborot tizimlarini uyali aloqa darajasida axborot xavfsizligini ta’minlash tizimi, Markaziy bankning markazlashgan antifrod hamda zamonaviy biometrik identifikatsiya tizimlariga ulanishini ta’minlash;

dasturlarni ishlatish bo‘yicha yo‘riqnomalarni ishlab chiqish va ularning aktualligini ta’minlagan holda mijozlarga taqdim etish;

aniqlangan zaifliklarni bartaraf etish uchun o‘zgarishlar kiritilishini ta’minlash;

mijozlar qo‘llayotgan dasturlarning aktualligini nazorat qilish.

To‘lov tizimlari operatorlari yoki to‘lov xizmatlarini yetkazib beruvchilar masofaviy axborot tizimlarining yangi talqinini (versiyasini) joriy etganidan so‘ng eski talqindan (versiyadan) foydalanishni cheklashi va yangi talqinga (versiyaga) o‘tishi (yangilashi) lozim.

9. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar o‘zaro to‘lov axborotlari va to‘lov axborotlariga tegishli bo‘lgan ma’lumotlar almashinuvini telekommunikatsiya tarmoqlari orqali amalga oshirish uchun tomonlarning axborotlashtirish obyektlari xususiyatlaridan kelib chiqib, ularning vazifalari, javobgarliklari va mazkur Nizom talablarini o‘z ichiga olgan axborot xavfsizligi va kiberxavfsizligini ta’minlash, shuningdek bank kartalari bilan bog‘liq shubhali (frod) operatsiyalarga qarshi choralar ko‘rish qoidalarini ishlab chiqishi kerak.

10. To‘lov agenti tomonidan bank yoki to‘lov tashkiloti bilan to‘lov xizmatlarini ko‘rsatish uchun tuzilgan agentlik shartnomasida axborot xavfsizligi bo‘yicha tomonlarning mas’uliyatlari belgilangan bo‘lishi kerak.

11. To‘lov subagenti tomonidan to‘lov agenti bilan to‘lov xizmatlarini ko‘rsatish bo‘yicha tuzilgan subagentlik shartnomasida axborot xavfsizligi bo‘yicha tomonlarning mas’uliyatlari belgilangan bo‘lishi kerak.

3-bob. To‘lov axborotlarining konfidensialligi hamda ulardagi shaxsga doir ma’lumotlarni himoya qilish

12. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar axborotning konfidensialligi va yaxlitligini, shu jumladan, to‘lov xizmatlaridan foydalanuvchining shaxsiga doir

ma’lumotlarni muhofaza qilishda hamda yetarli xavfsizlikni ta’minlash maqsadida quyidagi choralarni ko‘rishlari lozim:

to‘lov tizimida ishlov beriladigan konfidensial va shaxsga doir ma’lumotlarning yaxlitligi va daxlsizligini muhofaza qilish hamda ulardan foydalanish tartibini ishlab chiqish;

ichki hujjatlar bilan tartibga solinadigan himoyalanadigan ma’lumotlar bilan ishlashda xavfsizlik va konfidensiallikni ta’minlash qoidalari va talablarini ishlab chiqish;

konfidensial va shaxsga doir ma’lumotlar bilan ishlovchi xodimlar sonini imkon darajasida kamaytirish, xodimlar bilan konfidensial va shaxsga doir ma’lumotlar oshkor etilishining oldini olish bo‘yicha majburiyatnomalar (shartnoma) tuzish va ushbu ma’lumotlardan foydalanish huquqlarini xodimlarning lavozim majburiyatlaridan kelib chiqib belgilash;

konfidensial ma’lumotlar ro‘yxatini yuritish bo‘yicha komissiya tarkibini shakllantirish va tasdiqlash;

konfidensial ma’lumotlar ro‘yxati va hajmini aniqlash hamda tasdiqlash;

konfidensial ma’lumotlar bilan ishlashga ruxsat berilgan xodimlar ro‘yxatini shakllantirish va tasdiqlash;

axborotlashtirish obyektining texnik pasportini ishlab chiqish va tasdiqlash;

konfidensial ma’lumotlar bilan ishlash tartibini ishlab chiqish va tasdiqlash;

konfidensial ma’lumotlarni tashuvchi vositalarni ro‘yxatga olish, yo‘q qilish, konfidensial axborot tashuvchilarni tashqariga olib chiqish/kirish jurnallari yuritish;

ma’lumotlar yaxlitligi va xavfsizligini ta’minlash maqsadida elektron raqamli imzo kalitlaridan foydalanish hamda shifrlangan ma’lumotlarni saqlash tartibini belgilash;

konfidensial va shaxsga doir ma’lumotlar mavjud bo‘lgan resurslarga kirishda identifikatsiya, autentifikatsiya va avtorizatsiya qilinishini ta’minlash;

konfidensial va shaxsga doir ma’lumotlar bilan ishlash huquqlarining ruxsatsiz berilishini oldini olish;

axborot tizimlari foydalanuvchilarining muhofazalangan ma’lumotlariga kirish, ishlov berish, ularni saqlash hamda taqdim etish jarayonidagi amalga oshirilgan harakatlarni elektron bayonnomalarda qayd etib borish;

tashqi saqlovchi qurilmalar va texnik vositalarning binodan tashqariga olib chiqilishi hamda ularning o‘g‘irlanishining oldini olish;

ma’lumotlarni uzatish, saqlash, o‘chirib tashlash, ularga ishlov berish hamda ularning ruxsatsiz chetga chiqib ketishining oldini olish choralari ta’minlanganligini nazoratga olish.

4-bob. Axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati

13. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar axborot tizimlarida axborot muhofazasi uchun axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati vazifalariga quyidagilarni kiritishlari lozim:

axborot tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha mazkur Nizom talablarining bajarilishini nazorat qilish;

axborot xavfsizligiga oid choralar ta’minlanganligini baholash, axborot xavfsizligi va kiberxavfsizlik darajasini oshirish, shuningdek avariyalar va xodimlarning yo‘l qo‘ygan xatolari natijasida kelib chiqadigan yo‘qotishlarni kamaytirish va ularning sodir etilishining oldini olish;

axborot infratuzilmasining yaxlitligi va xavfsizligini nazorat qilish;

serverlardagi dasturiy ta’minotlarni muhofaza qilish;

barcha texnologik jarayonlarda xodimlar harakatlari, shuningdek, axborot tizimlaridagi amalga oshirilgan to‘lov xizmatlaridan foydalanuvchilarining harakatlari bo‘yicha elektron bayonnomalar ro‘yxatini yuritish;

avtomatlashtirilgan tizimlarda kiberxavfsizlikni va noqonuniy harakatlar bilan mablag‘larni o‘zlashtirishning oldini olish choralarini ko‘rish;

ma’lumotlar uchinchi shaxslarga oshkor etilishining oldini olish choralarini ko‘rish;

axborot kommunikatsiya texnologiyalari infratuzilmasida yuzaga kelgan axborot xavfsizligi va kiberxavfsizlik hodisalari, kibertahdidlar, kiberhujumlar aniqlangan vaqtda bu haqidagi ma’lumotlarni Markaziy bankka taqdim etish;

axborot kommunikatsiya texnologiyalari infratuzilmasi, axborot tizimlari va resurslarida axborot xavfsizligi va kiberxavfsizlikning ta’minlanganlik holatining mazkur Nizom talablari, ichki qoida va tartiblarga muvofiqligini bir yilda kamida ikki marotaba axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini hisobga olgan holda o‘rganish va o‘rganish natijalarini dalolatnoma bilan rasmiylashtirish.

5-bob. Axborot tizimlarida xodimlarning vakolatlarini cheklash

14. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar axborot tizimlarida ishlash jarayonida, shu jumladan, ishlab chiqish, sinovdan o‘tkazish jarayonida xodimlarning vakolatlarini chegaralash uchun quyidagi choralarni ko‘rishlari lozim:

axborot tizimlarida ishlash huquqlarini belgilovchi tartib va qoidalarni ishlab chiqish va ularni lavozim yo‘riqnomalarida aks ettirish hamda tegishli hujjatga (ariza, talabnoma yoki boshqa shaklga) asosan tizimdan foydalanish tartibini ta’minlash;

axborot tizimlarida ishlash huquqi berilgan mas’ul xodimlar ro‘yxatini shakllantirish;

axborot tizimlarida ishlash huquqlarini belgilash va taqsimlash bilan bog‘liq harakatlarni ro‘yxatga olish;

axborot tizimlarida ishlash huquqlari mantiqan, ish vazifasidan kelib chiqib to‘g‘ri belgilanganligini davriy (yiliga kamida ikki marotaba) tekshirib turish;

axborot tizimlarining ishlashi va sinovdan o‘tkazilishi davrida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda berilgan axborot tizimlarida ishlash huquqlari to‘g‘riligini nazorat qilish;

axborot tizimi foydalanuvchilari axborot tizimi tomonidan berilgan huquqlarni o‘zgartirish imkoniyatiga ega bo‘lmasligi hamda bu huquqlarni begona shaxslarga berishni cheklash choralarini ko‘rish.

15. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar o‘zlarining axborot tizimlariga o‘zgartirishlar kiritish uchun boshqa tashkilotlarni jalb qilganda quyidagilarni amalga oshirishlari zarur:

konfidensial va shaxsga doir ma’lumotlarni oshkor etmaslik bo‘yicha bitim tuzish;

axborot tizimlaridagi to‘lovlarga oid va boshqa muhofaza qilinadigan ma’lumotlar bilan ishlashni belgilangan tartibda ruxsat berish asosida amalga oshirish;

tegishli litsenziya va (yoki) boshqa ruxsatnomaga ega bo‘lgan (agar ushbu faoliyat litsenziya yoki tegishli ruxsatnoma asosida amalga oshirilsa) tashkilotlarni jalb qilish;

axborot tizimlarini loyihalashtirish bosqichida ma’lumotlarning konfidensialligini ta’minlash choralarini ishlab chiqish;

ko‘riladigan axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha choralar (amalga oshiriladigan ishlar, o‘rnatiladigan dasturlar, qurilmalar va boshqalar), aniq ko‘rsatilgan texnik topshiriq, qabul qilish (test sinovlarini amalga oshirish rejasi) va boshqa tegishli hujjatlarni rasmiylashtirish;

dasturiy ta’minot hamda uni ishlab chiqqan va unga o‘zgartirish kiritgan (kiritadigan) tashkilotlar ro‘yxatini tuzish;

axborot tizimlarini ishlab chiqish va joriy etishning taxminiy muddatlarini va shartlarini belgilab olish;

jalb qilingan tashkilot xodimlari tomonidan axborot tizimlariga kiritiladigan o‘zgartirishlarning asosliligini, mavjud texnik topshiriqlarga mosligini, axborot tizimiga yot bo‘lgan dasturlar (tizim funktsiyalari) bo‘lmasligini, test sinovlari natijalarining ijobiyligini axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati hamda axborotlashtirish bo‘yicha mas’ul xodim tomonidan nazoratga olish.

Avtomatlashtirilgan tizimlarga o‘zgartirish kiritgan tashkilot o‘z vazifasini amalga oshirganidan so‘ng yoki u bilan tuzilgan shartnoma muddati tugaganida, unga ma’lum bo‘lgan barcha konfidensial ma’lumotlar (identifikator, parollar va boshqalar) hamda tizimga kirish imkoniyatlari axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati tomonidan o‘zgartirilishi lozim.

6-bob. Axborot tarmoqlarini hujumlardan himoya qilish

16. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar axborot va internet jahon axborot tarmog‘ini, shuningdek, serverlar va aloqa kanallarini ehtimoli mavjud bo‘lgan kibertahdid va kiberhujumlardan himoya qilish uchun yetarli choralarni ko‘rishi lozim. Ushbu choralar quyidagilarni o‘z ichiga olishi kerak:

kompyuter tarmoqlarini segmentlash va tarmoqlararo ekrandan foydalanish;

axborot tarmoqlari, shu jumladan, internet jahon axborot tarmog‘i orqali qabul qilinayotgan va uzatilayotgan ma’lumotlarga ruxsatsiz kirishning oldini olish bo‘yicha texnik (kriptografik va boshqa) va/yoki tashkiliy choralar ko‘rish hamda tarmoq ma’lumotlarini filtrlashni ta’minlash (tarmoqlararo ekranlarni qo‘llash);

axborot tarmoqlari va veb-saytlar orqali to‘lovlarni amalga oshirishda identifikatsiya, ko‘p omilli autentifikatsiya va avtorizatsiya qilish (ko‘p omilli autentifikatsiya qilish mobil va aloqasiz to‘lovlarni amalga oshirish chog‘ida qo‘llanilmaydi);

axborot tarmoqlari va Internet jahon axborot tarmog‘i, shuningdek, serverlar va aloqa kanallaridan foydalanuvchilarni identifikatsiya qilish;

internet jahon axborot tarmog‘i resurslaridan xodimlarning foydalanishini proksi-server orqali amalga oshirish, ish faoliyati uchun zarur bo‘lmagan veb-saytlarga kirishni chegaralash va kirilgan veb-saytlarni qayd

etib borish;

axborot tizimlarini asosiy va zaxira aloqa kanallari bilan ta’minlash;

serverlar tarmog‘ini muhofazalash (demilitarizatsiya qilingan zonalarini (DMZ) tashkil etish);

serverlarda ish faoliyati uchun zarur bo‘lmagan portlarni yopish va xizmatlarni to‘xtatish;

axborot tizimiga kirish obyektlari va resurslarining hisobini yuritish;

mobil to‘lovlarni amalga oshirish chog‘ida foydalanuvchilarni ko‘p faktorli autentifikatsiya qilish (SMS, QR-kod, NFC, barmoq izlari, ko‘zning rangdor pardasi asosida aniqlash yoki shu kabi tasdiqlovchi usullarni qo‘llash mumkin);

mobil qurilmalar yordamida masofadan kirishda to‘lov ma’lumotlari hamda axborot tizimlarining (ma’lumotlar bazasining) axborot xavfsizligi va kiberxavfsizligini ta’minlash;

masofaviy xizmat ko‘rsatish va boshqa axborot tizimlarida mijozni identifikatsiya va autentifikasiya qilish maqsadida qo‘llaniladigan (bir martalik yoki ko‘p martalik) parollarni ishlatish tartibini belgilash, tasdiqlash kodlarini qo‘llash, bir martalik tasdiqlash kodlarini tizimga shifrlangan holda yuborish, antifrod va biometrik identifikatsiya tizimlarini qo‘llash, kodning faol bo‘lish vaqti va boshqalarni yoritish;

avtomatlashtirilgan tizimga kirishda qo‘llanilgan qurilma to‘g‘risida identifikatsiya ma’lumotlarini (IP-adres, MAC-adres va boshqa identifikatorlar) qayd etish;

tajovuzlarni aniqlash va ularning oldini olish tizimlarini qo‘llash.

17. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar chet el tashkilotlarining axborot muhofazasi uskunalarini qo‘llashlari mumkin.

18. To‘lov tizimlari operatorlari to‘lovlar bilan bog‘liq axborot almashinuvi uchun qo‘llaniladigan texnik va tashkiliy choralarni, ish tartiblarini belgilashi hamda ushbu tartiblar ijrosi to‘lov xizmatlarini yetkazib beruvchilar tomonidan ta’minlanishi lozim.

19. Axborot xavfsizligi va kiberxavfsizligini kuchaytirish maqsadida tarmoq protokolida (TCP/IP) tarmoq tranzit paketlarining IP manzillarini o‘zgartirish imkonini beruvchi tarmoq adreslarini o‘zgartirish protokoli (NAT) qo‘llanilishi mumkin. Bunda tarmoq orqali barcha ulanishlarning elektron jurnallari asl IP manzillar ko‘rsatilgan holda yuritilishi va belgilangan tartibda elektron arxivga olinishi lozim.

20. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar ichki hujjatlarida quyidagilarni belgilashlari lozim:

axborot tarmoqlarini xavfsiz va ishonchli aloqa kanallari bilan ta’minlash tartibi;

to‘lov tizimiga kirish va undan chiqish jarayoni tartibi;

foydalanuvchini to‘lov tizimiga ulashda axborot xavfsizligi va kiberxavfsizlikni ta’minlash tartibi;

axborot xavfsizligi va kiberxavfsizlik hodisasi, kibertahdid hamda kiberhujumlar bilan bog‘liq tavakkalchiliklarni baholash va boshqarish tartibi;

protsessing va kliring jarayonlarida axborot xavfsizligi tartibi va talablari (agar ushbu xizmat amalga oshirilsa);

xatarlarni boshqarish choralari va usullari;

avtomatlashtirilgan tizimda, axborot dasturlarida foydalanuvchilarning yagona identifikatorini hosil qilish tartibi;

qayd etiladigan harakatlar ro‘yxati;

ma’lumotlarni ro‘yxatga olish va saqlash tartibi.

7-bob. Axborot tizimlari va resurslari monitoringi

21. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar to‘lovlar bo‘yicha konfidensial ma’lumotlardan va o‘ta muhim mantiqiy hamda jismoniy resurslardan (axborot tarmoqlari, axborot tizimlari, ma’lumotlar bazalaridan, axborotni himoya qilish modullaridan) foydalanish monitoringini amalga oshiradi. Bunda monitoring qilishda quyidagilar belgilanadi:

axborot infratuzilmasining axborotga ishlov berish, ularni saqlash va tarmoqda uzatish uchun qo‘llaniladigan dastur va qurilmalar hisobini yuritish;

axborot xavfsizligi va kiberxavfsizlik hodisalarini tahlil qilish, axborot xavfsizligi va kiberxavfsizlik holatini monitoring qilish hamda ogohlantirish imkonini beruvchi (Security Information and Event Management (SIEM) yoki boshqalar) tizimlarni joriy qilish;

axborot xavfsizligi va kiberxavfsizligi holatini monitoring qilishni amalga oshiruvchi tizim ma’lumotlarini tahlil qilib borish va aniqlangan holatlarni (axborot tarmog‘iga ruxsatsiz kirish va kirishga urinish, tizimdagi to‘xtalishlar, axborot resurslarining yetishmovchiligi, tarmoqdagi uzilishlar, axborot xavfsizligi va kiberxavfsizligini ta’minlashdagi cheklanishlar va boshqa hodisalar) bartaraf etish va (yoki) ularning oldini olish bo‘yicha choralar ko‘rish;

konfidensial ma’lumotlardan va o‘ta muhim mantiqiy hamda jismoniy resurslardan (axborot tarmoqlari, axborot tizimlari, ma’lumotlar bazalaridan, axborotni himoya qilish modullaridan) ruxsatsiz foydalanishning oldini olish bo‘yicha choralar ko‘rish;

foydalanuvchi operatsiyani amalga oshirgan sana (kun, oy, yil) va vaqt (soat, daqiqa, soniya), uning amalga oshirgan operatsiyasi foydalanuvchiga avtomatlashtirilgan tizimlarda hamda axborot dasturlarida berilgan identifikatsiya raqami, tizimlarga kirishda mavjud bo‘lgan identifikatsiya ma’lumotlari (IP-adres, MAC-adres, IMEI-kod, telefon raqami va/yoki qurilmaning boshqa identifikatori), avtomatlashtirilgan tizimlar tomonidan foydalanuvchiga huquq berilishi bilan bog‘liq harakatlarni qayd etish;

axborot xavfsizligi va kiberxavfsizlik holatini tun-u kun (24/7) rejimida monitoring qilish ishlarini tashkil etish;

axborot xavfsizligi va kiberxavfsizligi holatini monitoring qilish tizimini Markaziy bank “CERT-CBU” kiberxavfsizlik markazining monitoring tizimiga bog‘lanishini ta’minlash;

axborot dasturlari, avtomatlashtirilgan tizimlar ishlatilishi bilan bog‘liq foydalanuvchilarning harakatini (operatsiya) qayd etish.

8-bob. Axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalarni aniqlash

22. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar to‘lovlarni va pul mablag‘larini o‘tkazishni amalga oshirish chog‘ida axborot xavfsizligi va kiberxavfsizlikni ta’minlashga doir talablarning buzilishi bilan bog‘liq bo‘lgan hodisalarni aniqlash maqsadida axborot xavfsizligi va kiberxavfsizlikni ta’minlashga doir tashkiliy choralarni ko‘rishda hamda texnik vositalarni qo‘llashda quyidagi

ishlarni tashkil etishi lozim:

qo‘llanilishi zarur bo‘lgan axborot xavfsizligi va kiberxavfsizlik bo‘yicha tashkiliy choralarni aniqlash;

mavjud texnik qurilmalarni ishlatish, sozlash hamda ulardagi ma’lumotlarni qayd etish bo‘yicha mas’ul xodimlarni tayinlash;

axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalarni aniqlash choralarini ko‘rish hamda ushbu holatlar xodimlar tomonidan aniqlanganda ularning axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmatini xabardor qilishi;

axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalar yuzaga kelganda ularni bartaraf etish, yuzaga kelish sabablarini aniqlash, tahlil qilish hamda aniqlangan hodisalar yuzaga kelmasligi bo‘yicha tegishli choralar ko‘rish;

aniqlangan hodisalarni ro‘yxatga olib borish (reyestrini yuritishi);

aniqlangan hodisalar to‘g‘risidagi ma’lumotlarni saqlash tartibini belgilash;

axborot xavfsizligi va kiberxavfsizligini ta’minlashning boshqa choralarini ko‘rish.

To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalar to‘g‘risida Markaziy bankka zudlik bilan yozma yoki elektron shaklda xabar berishi lozim.

23. To‘lov tizimlari operatorlari axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalarning oldini olish maqsadida, quyidagi talablarni belgilashi kerak:

to‘lov tizimining boshqa ishtirokchilariga to‘lovlarni amalga oshirish uchun zarur texnik va dasturiy vositalarga axborot xavfsizligi va kiberxavfsizlik bo‘yicha qo‘yiladigan talablarni;

to‘lov tizimi va to‘lovlar bilan bog‘liq noxush hodisalar to‘g‘risida ma’lumot berish shakli va tartibiga bo‘lgan talablarni;

to‘lov tizimida axborot xavfsizligi va kiberxavfsizligiga oid tavakkalchiliklarni boshqarish tartibi va ularni baholash mezonlarini;

to‘lovga oid ma’lumotlarga ishlov berish vositalarining xavfsiz ishlashini ta’minlash tartibini;

to‘lov tizimida noxush hodisalar yuzaga kelganda o‘zaro harakatlanish tartibini.

24. To‘lov xizmatlarini yetkazib beruvchilar axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalarning oldini olish maqsadida quyidagi talablarni belgilashi kerak:

to‘lovni amalga oshirish qurilmalarini mijozga yetkazib berish bilan bog‘liq tavakkalchiliklarning oldini olish choralarini ko‘rish;

to‘lov uskunalarining yo‘qolishi, o‘g‘irlanishi, begona shaxslar tomonidan egalik qilinishi kabi holatlar aniqlanganda to‘lov tizimlari operatorlariga xabar berishi lozim.

25. To‘lov tizimi operatorlari tomonidan to‘lov xizmatlarini yetkazib beruvchilarga to‘lov tizimida axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalar to‘g‘risida ma’lumot berilishi hamda ushbu holatni tahlil qilish va bartaraf etish bo‘yicha uslubiy qo‘llanma taqdim qilinishi lozim.

9-bob. Axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalarga nisbatan

ta’sir choralari

26. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha talablarning buzilishi bilan bog‘liq bo‘lgan hodisalarga nisbatan quyidagi ta’sir choralarini ko‘rishlari lozim:

yuzaga kelishi mumkin bo‘lgan hodisalarga nisbatan ta’sir choralarini ko‘rish yuzasidan zarur harakatlarni oldindan ko‘ra bilish hamda amalga oshiriladigan harakatlar ro‘yxatini belgilash;

sodir bo‘lgan hodisalarga nisbatan qisqa muddatlarda ta’sir choralarini ko‘rish;

ishning uzluksizligini ta’minlash, shuningdek, noqonuniy to‘lovlar va hisobvaraqlardagi qoldiq mablag‘larini ruxsatsiz o‘zgartirilishini oldini olish, axborotni qayta tiklash hamda boshqa salbiy holatlarni bartaraf etish;

xodimlar tomonidan mavjud axborot tizimlarida ishlashda belgilangan axborot xavfsizligi va kiberxavfsizlik talablariga rioya qilinishini ta’minlash;

yuzaga kelgan hodisalarning kelib chiqish omillarini aniqlash maqsadida tarmoq qurilmalari va axborot tizimlarining elektron bayonnomalarini rasmiylashtirish, yig‘ish, tahlil qilish hamda ularga asosan tegishli ko‘rsatmalarni ishlab chiqish.

10-bob. Axborot xavfsizligi va kiberxavfsizlik talablarining buzilishi bilan bog‘liq hodisalar sabablarini tahlil qilish

27. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar axborot xavfsizligi va kiberxavfsizlikni ta’minlashga doir talablarning buzilishi bilan bog‘liq aniqlangan hodisalar sabablarini tahlil qilishi hamda ularga ta’sir ko‘rsatish natijalarini baholashi lozim. Bunda aniqlangan hodisalar sabablarini tahlil qilish hamda ularga ta’sir ko‘rsatish natijalarini baholash tizimi quyidagilarni o‘z ichiga olishi lozim:

aniqlangan hodisalarga nisbatan ta’sir choralari ko‘rilgandan keyin ushbu hodisalarning kelib chiqish sabablarini axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati tomonidan tegishli bo‘linmalar bilan birgalikda tahlil qilish tartibi;

axborot tizimlarining tegishli elektron bayonnomalarini o‘rganish hamda aniqlangan hodisaning yuzaga kelishiga sababchi bo‘lgan xodimlardan tushuntirishlar olish;

hodisalarning kelib chiqish sabablariga oydinlik kiritib, bunday holatlar yuzaga kelmasligi yoki yuzaga kelganda uning zarar keltirish imkoniyatlarini kamaytirish choralarini ko’rish (shu jumladan, tegishli mutaxassislarni jalb qilgan holda);

hodisalarning salbiy ta’sir ko‘rsatish darajasiga qarab tasniflash va baholash mezoniga asosan ularni baholash.

Axborot xavfsizligi va kiberxavfsizlikni ta’minlashga doir talablarning buzilishi bilan bog‘liq aniqlangan hodisalarga nisbatan ko‘rilgan ta’sir choralari, ularni baholash natijalari va boshqa qo‘shimcha ma’lumotlar chop etilishi hamda alohida yig‘majildda saqlanishi zarur.

11-bob. Bankomat, infokiosk va to‘lov terminallarini qo‘llashda axborot xavfsizligi va kiberxavfsizlikni

ta’minlash

28. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar bankomat, infokiosk va to‘lov terminallarining axborot xavfsizligi va kiberxavfsizligini ta’minlashi lozim. Bunda axborot xavfsizligi va kiberxavfsizlikni ta’minlashda quyidagi choralar qo‘llaniladi:

bankomat, infokiosk va to‘lov terminallarining hisobini yuritish hamda ularning axborot dasturiga ruxsatsiz kirishining oldini olish;

bankomat, infokiosk va to‘lov terminallariga texnik xizmat ko‘rsatuvchi shaxslar faoliyatini nazorat qilish hamda ular tomonidan amalga oshirilgan o‘zgartirishlar bo‘yicha elektron bayonnoma yuritish;

videokuzatuv tizimlari yordamida bankomatlar bilan ishlash jarayonlarini nazoratga olish (bankomatga kiritiladigan bank kartalarining pin kod raqamlari videokuzatuv tizimlari orqali qayd etish imkoniyatiga ega bo‘lmasligi lozim);

bosh bank hamda uning infratuzilmalari (filial, mini-bank va boshqalar) va boshqa qo‘riqlanadigan obyektlaridan tashqarida joylashtirilgan bankomatlarning videokuzatuv ma’lumotlari bosh bank yoki uning filialidagi texnik qurilmalarga to‘g‘ridan to‘g‘ri (onlayn) yozib borilishini ta’minlash;

bankomat tarmoq kabellarini muhofazalash;

bankomatning boshqa bankomatlar bilan bir xil bo‘lgan qulflarini almashtirish;

bankomatlarni aloqa kanallaridan yoki jismonan bog‘langan holda ehtimoliy hujumlardan (shu jumladan, skimmingdan) himoya qilish;

bankomatlarning operatsion tizimi hamda BIOS tizimiga kirish huquqlarini murakkab parollar bilan himoyalash;

autentifikatsiya qilish tartibini belgilash;

to‘lovlarni amalga oshiruvchi qurilmalarning hisobini yuritish;

bankomatlardagi naqd pul mablag‘larining jismoniy muhofazasini ta’minlash;

tarmoq orqali axborot almashinuvida axborot xavfsizligi va kiberxavfsizlikni ta’minlash;

xalqaro to‘lov tizimlari bilan ishlaydigan axborot tizimlarida xalqaro standartlar (PCI DSS, PTS, PA DSS) talablariga muvofiq axborot muhofazasi vositalari va tizimlarini joriy qilish.

29. To‘lov tizimlari operatorlari o‘z tizimlaridagi bankomat va infokiosklarda axborot xavfsizligi va kiberxavfsizlikni banklar bilan birgalikda ta’minlaydi hamda ularning uzluksiz va to‘g‘ri ishlashini nazorat qiladi. Agar axborot xavfsizligi va kiberxavfsizlik bo‘yicha ma’lum bir (yoki barcha) mas’uliyat to‘lov xizmatlarini yetkazib beruvchiga yuklatilgan bo‘lsa, mazkur holat tegishli shartnomalarda qayd etilishi va mas’uliyat yuklatilgan tashkilotga zaruriy sharoitlar yaratib (bankomatlarning axborot tizimidagi ishlash huquqlari) berilishi zarur.

12-bob. Muhim to‘lov tizimlari operatorlariga axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha qo‘yiladigan talablar

30. Muhim to‘lov tizimlari operatorlari mazkur Nizomda belgilangan xavfsizlik choralariga

qo‘shimcha ravishda quyidagi axborot xavfsizligi va kiberxavfsizlik choralarini ta’minlashi zarur:

to‘lov tizimining uzluksiz ishlashi ishonchliligini ta’minlash;

axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmatini tashkil etish va uning majburiyatlarini belgilash;

O‘z DSt 2875:2014 “Datamarkazlarga qo‘yiladigan talablar. Infratuzilma va axborot xavfsizligini ta’minlash” standartining datamarkaz telekommunikatsiya vositalari infratuzilmasi tayyorligi va xavfsizligining uchinchi darajadan past bo‘lmasligini ta’minlash;

xalqaro bank kartalaridan foydalanilganda PCI DSS xavfsizligi standarti, Payment Services Directive (PSD2) to‘lov xizmatlarini ko‘rsatish direktivasi talablariga muvofiqlashtirish;

axborot tizimlari to‘g‘ri tashkil etilganligi yuzasidan nufuzli xalqaro auditor tashkilotlarni jalb qilish orqali AKT-infratuzilmasini (axborot xavfsizligi holatini) auditdan o‘tkazishni ta’minlash;

O‘zbekiston Respublikasining “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonuni va boshqa qonunchilik hujjatlarida muhim to‘lov tizimlari operatorlariga belgilangan talablarni bajarish.

31. Muhim to‘lov tizimlari operatorlari ma’lumotlarga ishlov beruvchi asosiy axborot tizimlarini tashkil etishi va joylashgan joyidan 50 kilometrdan yaqin bo‘lmagan hududda zaxira axborot tizimlarini tashkil etishi lozim. Bunda asosiy va zaxira axborot tizimlari O‘zbekiston Respublikasi hududida tashkil etiladi.

Muhim to‘lov tizimlari operatorlarining axborot tizimlaridagi ma’lumotlarni (elektron bayonnomalar va boshqa to‘lovlar bilan bog‘liq ma’lumotlar) elektron arxivlarda kamida ikki nusxada (xususan, asosiy va zaxira axborot tizimlarining har birida bitta nusxadan) saqlashi lozim.

13-bob. To‘lov tizimining uzluksiz ishlashini yo‘lga qo‘yish va elektron arxiv yuritish

32. To‘lov tizimlarining uzluksiz ishlashi va barqarorligini ta’minlash maqsadida quyidagi choralar ko‘rilishi lozim:

to‘lov tizimi bilan bog‘liq tarmoq va boshqa qurilmalar nosoz holatga kelganda uni ish jarayoniga keltirish va uzluksiz ishlashini ta’minlash;

operatsion tizim, dasturiy ta’minotlar, axborot tizimlarining dasturlari, ma’lumotlar (ma’lumotlar bazasi, sozlamalari, elektron bayonnomalar) nusxalarini zaxiraga (backup) olinishi va elektron arxivda saqlash hamda ularni qayta tiklash tartibini (mexanizmini) ishlab chiqish, ularning hisobini yuritish va nazoratini olib borish;

zaxira texnik qurilma va uskunalarga ega bo‘lish;

ma’lumotlarning zaxiraga olingan (backup) nusxalarini texnik nosozliklarda va favqulodda vaziyatlarda qayta tiklash rejasini ishlab chiqish va davriy (bir yilda bir marotaba) axborot tizimini qayta tiklab tekshirish;

dasturlarga o‘zgarish kiritishni sinov (test) uchun mo‘ljallangan serverlarda tekshirish;

tizimdagi qurilma va uskunalarning ishlashini nazorat qilish;

to‘lov tizimining uzluksizligiga salbiy ta’sir etishi mumkin bo‘lgan holatlarni oldini olish va axborot muhofazasini ta’minlash;

dizel elektr stansiyasi va/yoki boshqa elektr ta’minoti uzluksizligini ta’minlash vositalaridan (UPS va boshqalar) foydalanish;

ishlov berilgan ma’lumotlarni saqlash va ularning elektron arxivda yuritilishini ta’minlash;

mijozlarning harakatiga tegishli bo‘lgan ma’lumotlarni kamida besh yil saqlanishini ta’minlash;

elektron arxiv yuritishda axborot xavfsizligi va kiberxavfsizlikni ta’minlashga doir talablarga rioya etilishi bo‘yicha ishchi guruh tuzgan holda bir yilda kamida ikki marotaba tekshirish va natijalari to‘g‘risida Markaziy bankka ma’lumot berish;

axborot uzatish zaxira tarmoqlariga ega bo‘lish.

33. Muhim to‘lov tizimlari operatorlari bo‘lmagan to‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar ma’lumotlarga ishlov beruvchi asosiy axborot tizimlarini tashkil etishi va ular joylashgan joyidan 5 kilometrdan yaqin bo‘lmagan hududda zaxira axborot tizimlarini tashkil etishi lozim. Bunda asosiy va zaxira axborot tizimlari O‘zbekiston Respublikasi hududida tashkil etiladi.

Axborot tizimlaridagi ma’lumotlar (elektron bayonnomalar va boshqa to‘lovlar bilan bog‘liq ma’lumotlar) elektron arxivlarda kamida ikki nusxada (xususan, asosiy va zaxira axborot tizimlarining har birida bitta nusxadan saqlanishi mumkin).

34. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning faoliyati tugatilganda, ulardagi mavjud elektron arxivning axborot resurslari davlat arxivlariga topshiriladi.

To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar faoliyati tugatilib, boshqa tashkilotga qo‘shib yuborilganda, elektron arxiv ma’lumotlari qo‘shib yuborilayotgan tashkilotning elektron arxivga topshiriladi.

14-bob. Xavfsizlik rejimi

35. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lovlar bilan bog‘liq ma’lumotlarni saqlash va ularga ishlov berish xonalari bilan ta’minlangan bo‘lishi kerak. Ushbu xonalar quyidagi talablarga javob berishi lozim:

ruxsatsiz jismoniy kirishdan muhofazalangan bo‘lishi;

xona birinchi qavatda joylashgan hollarda uning derazalari temir panjara bilan jihozlangan bo‘lishi;

qo‘riqlash va yong‘indan ogoh etuvchi ikkita himoya to‘sig‘i xabargohlari bilan jihozlanishi;

tungi vaqtda qo‘riqlash va ogohlantirish qurilmalari bilan jihozlanishi;

videokuzatuv orqali nazoratga olinishi.

To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar to‘lovlar bilan bog‘liq ma’lumotlarni saqlash va ularga ishlov berish xonalarini mazkur bandda belgilangan talablardan tashqari boshqa xavfsizlik choralarini ko‘rishi mumkin.

36. Mazkur Nizomda belgilangan barcha videokuzatuv ma’lumotlarining saqlanish muddati bir oydan kam bo‘lmasligi zarur.

37. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning binolari himoya qilinishida ular zaruriy uskunalar, tashkiliy-texnik vositalar bilan jihozlanishi va tegishli dasturiy

ta’minotlardan foydalanilishi lozim.

15-bob. To‘lovlarni amalga oshirish jarayonini nazorat qilish

38. To‘lov tizimlari operatorlari o‘zlarining to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlik choralarini ko‘rishda nazorat va monitoring ishlarini amalga oshirishlari lozim.

39. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar avtomatlashtirilgan tizimlar, ilovalar hamda axborot infratuzilma obyektlarini axborot xavfsizligi va kiberxavfsizlik zaifliklariga tahlil qilishi, har yili kamida ikki marta ruxsatsiz kirishga tekshirishi va hujjatlarda qayd etilmagan imkoniyatlar mavjud emasligini nazorat qilishi lozim.

40. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilar har yili, kelgusi yilning birinchi aprelidan kechiktirmay, Markaziy bankka axborot xavfsizligi va kiberxavfsizlikning ta’minlanganlik holati to‘g‘risida hisobot taqdim etishi shart.

16-bob. Bank va to‘lov tizimlarida shubhali frod operatsiyalarga qarshi choralar ko‘rish xizmati

41. To‘lov tizimlari operatorlari, to‘lov tizimining ishtirokchilari va to‘lov tashkilotlari bank va to‘lov tizimlarida shubhali (frod) operatsiyalarga qarshi choralar ko‘rish xizmati vazifalariga quyidagilarni kiritishlari lozim:

masofadan turib bank kartalari va hisobvaraqlari, mobil ilovalardagi akkauntlar hamda elektron hamyonlar bilan bog‘liq operatsiyalarni amalga oshiruvchi axborot tizimlarini (mobil ilova, internet banking va boshqalar) Markaziy bankning markazlashgan antifrod hamda biometrik identifikatsiya tizimlariga ulash;

pul mablag‘larini o‘tkazish bilan bog‘liq shubhali (frod) operatsiyalari ro‘yxatini yuritib borish;

bank kartalari va hisobvaraqlari, mobil ilovalardagi akkauntlar hamda elektron hamyonlar bilan bog‘liq shubhali (frod) operatsiyalarida ishtirok etgan bank kartalari to‘g‘risidagi ma’lumotlarni yig‘ib borish;

bank kartalari va hisobvaraqlari, mobil ilovalardagi akkauntlar hamda elektron hamyonlar bilan bog‘liq shubhali (frod) operatsiyalarini amalga oshirilishini antifrod tizimlari yordamida oldini olish;

bank kartalari bilan bog‘liq shubhali (frod) operatsiyalar sodir etilgan taqdirda, Markaziy bankning majburiy ko‘rsatmasiga asosan bank kartalari va hisobvaraqlari, mobil ilovalardagi akkauntlar hamda elektron hamyonlardan foydalanishni uch kungacha muddatga vaqtincha cheklashni (bloklashni) amalga oshirish;

bank kartalari va hisobvaraqlari, mobil ilovalardagi akkauntlar hamda elektron hamyonlar bilan bog‘liq shubhali (frod) operatsiyalarga qarshi choralarni ko‘rish xizmati (shubhali (frod) operatsiyalarga qarshi choralar ko‘rishga mas’ul xodimlari) faoliyatini tun-u kun (24/7) rejimida ishlashini tashkil etish;

masofadan turib bank kartalari va hisobvaraqlari, mobil ilovalar akkauntlari hamda elektron hamyonlar bilan bog‘liq operatsiyalarni amalga oshiruvchi axborot tizimlarini (mobil ilova, internet banking va boshqalar) antifrod hamda biometrik identifikatsiya tizimlari bilan bog‘liq holda uzluksiz ishlashini nazorat qilish.

17-bob. Jismoniy va yuridik shaxslarning roziligisiz to‘lovlar amalga oshirilishini oldini olish

42. To‘lov tizimi operatorlari, to‘lov tizimining ishtirokchilari va to‘lov tashkilotlari tavakkalchiliklarni boshqarish to‘g‘risidagi hujjatlarida jismoniy va yuridik shaxslarning roziligisiz amalga oshirilgan pul o‘tkazmalarining tavsifi, miqdori va harakatlarini tahlil etish orqali bank kartalaridan jismoniy va yuridik shaxslarning roziligisiz amalga oshirilgan pul o‘tkazmalarining mezonlariga mos keladigan operatsiyalarni aniqlash jarayonlarini belgilaydi.

43. To‘lov tizimi operatorlari bank kartalari orqali jismoniy va yuridik shaxslarning roziligisiz pul o‘tkazmalarini oldini olish maqsadida tranzaksion antifrod tizimlarini joriy etishi hamda Markaziy bankning markazlashgan antifrod tizimiga integratsiya qilinishini ta’minlashi lozim.

44. To‘lov tizimining ishtirokchilari va to‘lov tashkilotlari o‘zlarida session antifrod tizimlarini joriy etishi hamda Markaziy bankning markazlashgan antifrod tizimiga integratsiya qilinishini ta’minlashi lozim.

45. To‘lov tizimi ishtirokchilari va to‘lov tashkilotlarida bank kartalari orqali jismoniy va yuridik shaxslarning roziligisiz amalga oshirilgan pul o‘tkazmalarining mezonlariga mos keladigan operatsiyalar aniqlanganda, ushbu operatsiya bo‘yicha taqdim etilgan farmoyishning bajarilishini antifrod tizimlari doirasida amalga oshiradi.

46. To‘lov tizimi operatorlari, to‘lov tizimining ishtirokchilari va to‘lov tashkilotlari jismoniy va yuridik shaxslarning roziligisiz amalga oshiriladigan to‘lovlarni oldini olish maqsadida quyidagilarni bajarishi lozim:

jismoniy va yuridik shaxslarning roziligisiz amalga oshirilgan pul o‘tkazmalarining tavsifi, miqdori va harakatlarini tahlil etishi, tavakkalchiliklarni baholashi va boshqarishi hamda ularning mezonlariga mos keladigan operatsiyalarni aniqlash jarayonlarini belgilashi;

jismoniy va yuridik shaxslar o‘rtasida tuzilgan shartnomalarda (ommaviy ofertalarda) antifrod tizimi doirasida bank kartalari bilan bog‘liq shubhali (frod) operatsiyalarga qarshi choralar ko‘rish masalalarini yoritishi;

bank kartalari bilan bog‘liq shubhali (frod) operatsiyalar bo‘yicha kelib tushadigan murojaatlarni yig‘ishi va tahlil qilishi;

to‘lov xizmati foydalanuvchisining pul mablag‘larini o‘tkazish vaqtida, ushbu to‘lov shubhali (frod) operatsiyalar ro‘yxatida bo‘lsa, bunday holat haqida foydalanuvchiga xabar (SMS, messenjer yoki boshqa axborot tizimlar orqali) berishi, takroriy tasdiq (PIN kod, yashirin so‘zni kiritish yoki boshqa tarzda ma’lumot) olishi, agar ma’lum vaqt oralig‘ida ushbu tasdiq olinmasa, ushbu to‘lov operatsiyasini bekor qilishi;

foydalanuvchi tomonidan o‘zining hisob-varaqlariga tegishli to‘lov operatsiyalarini to‘xtatish (blokirovka qilish) imkoniyatini yaratishi;

bank kartalari bilan bog‘liq shubhali (frod) operatsiyalarda ishtirok etgan bank kartalari va hisobvaraqlari, mobil ilovalari akkauntlari hamda elektron hamyonlar to‘g‘risida o‘zlarining axborot tizimlarida mavjud bo‘lgan ma’lumotlarni Markaziy bankning so‘roviga asosan o‘z vaqtida taqdim etishi;

axborot tizimlari va resurslarida aniqlangan, jismoniy va yuridik shaxslarning roziligisiz amalga oshirilgan pul o‘tkazmalarini o‘tkazish yoki o‘tkazishga urinish holatlari to‘g‘risidagi ma’lumotlarni Markaziy bankka taqdim etib borishi.

47. To‘lov tizimi operatorlari, to‘lov tizimining ishtirokchilari hamda to‘lov tashkilotlari tomonidan jismoniy va yuridik shaxslarning roziligisiz to‘lovlar sodir etilgan holatlarda ishtirok etgan bank kartalari va

hisobvaraqlari, mobil ilovalari akkauntlari hamda elektron hamyonlardan foydalanishni vaqtincha cheklangan (bloklangan) muddat mobaynida qonun hujjatlarida ularni cheklash (bloklash) uchun boshqa asoslar bo‘lmaganda, ulardan foydalanishga qo‘yilgan vaqtinchalik cheklov (bloklash) olib tashlanadi.

48. Jismoniy va yuridik shaxslarning roziligisiz amalga oshirilgan pul o‘tkazmalarining mezonlari Markaziy bank boshqaruvining qaroriga asosan belgilanadi.

18-bob. EPOS-terminallaridan foydalanishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash

49. To‘lov tizimi operatorlari, to‘lov tizimining ishtirokchilari hamda to‘lov tashkilotlari EPOS-terminallaridan foydalanishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha quyidagilarni amalga oshirishi lozim:

to‘lov agentlari va subagentlarining reyestrini yuritishi, shuningdek, to‘lov agentlari yoki subagentlarini ro‘yxatdan o‘tkazish, o‘zgartirish va o‘chirishda 1 ish kuni ichida Markaziy bankka o‘zgartirilgan reyestrni taqdim etishi;

jismoniy shaxslar o‘rtasida pul mablag‘larini o‘tkazishni (P2P) amalga oshirish uchun alohida EPOS-terminalidan foydalanishi, shuningdek ushbu EPOS-terminallaridan boshqa maqsadlarda foydalanishini ta’qiqlashi;

EPOS-terminallaridan shartnomada ko‘rsatilgan maqsadlarda foydalanishni nazorat qilishi;

EPOS-terminallaridan, shuningdek foydalanuvchi parollari va kirish huquqlaridan foydalanishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash tartibini ishlab chiqishi.

50. To‘lov tizimi operatorlari va to‘lov tizimining ishtirokchilari Markaziy bankning majburiy ko‘rsatmasiga ko‘ra, shubhali (frod) operatsiyalari amalga oshirilishini cheklash yoki to‘xtatish maqsadida EPOS-terminallardan foydalanishni to‘xtatish yoki ushbu terminallarni o‘chirish choralarini ko‘rishi lozim.

19-bob. Yakuniy qoida

51. Mazkur Nizom talablarining buzilishida aybdor bo‘lgan shaxslar qonunchilik hujjatlarida belgilangan tartibda javobgar bo‘ladi.