O'ZBEKISTON RESPUBLIKASI
ADLIYA VAZIRLIGIDA
DAVLAT RO'YXATIDAN O'TKAZILDI
RO'YXAT RAQAMI: 3669
2025 - yil 18 - Avgust

O‘ZBEKISTON RESPUBLIKASI MARKAZIY BANKI BOSHQARUVINING QARORI

O‘zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga doir 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. O‘zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga doir minimal talablar to‘g‘risidagi nizom 1-ilovaga muvofiq tasdiqlansin.

2. Ayrim idoraviy normativ-huquqiy hujjatlar 2-ilovaga muvofiq o‘z kuchini yo‘qotgan deb topilsin.

3. Mazkur qaror O‘zbekiston Respublikasi Davlat xavfsizlik xizmati, Raqamli texnologiyalar vazirligi va Adliya vazirligi bilan kelishilgan.

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

O‘zbekiston Respublikasi
Markaziy banki Raisi
01-Avgust 2025-yil
19/1 son

ISHMETOV TIMUR
AMINDJANOVICH

Kelishildi:

O`zbekiston Respublikasi DXX
Raisi
18-Iyul 2025-yil

KURBANOV BAXODIR
NIZAMOVICH

Vazir
11-Iyul 2025-yil

SHERMATOV SHERZOD
XOTAMOVICH

Vazir
05-Iyul 2025-yil

TASHKULOV AKBAR
DJURABAYEVICH

O‘zbekiston Respublikasi
Markaziy banki boshqaruvining
2025-yil 1-avgustdagi
19/1-son qaroriga
1-ILOVA

O‘zbekiston Respublikasi tijorat banklarining axborot xavfsizligi va kiberxavfsizligiga doir minimal talablar to‘g‘risidagi NIZOM

Mazkur Nizom O‘zbekiston Respublikasi tijorat banklarining, shu jumladan mikromoliya banklarining (bundan buyon matnda bank deb yuritiladi) axborot xavfsizligi va kiberxavfsizligiga doir minimal talablarni belgilaydi.

1-bob. Umumiy qoidalar

1. Ushbu Nizomda quyidagi asosiy tushunchalar va qisqartmalardan foydalaniladi:

avtomatlashtirilgan bank tizimi – bank faoliyati sohasida axborotni to‘plash, saqlash, izlash, unga ishlov berish va undan foydalanishni amalga oshirish uchun mo‘ljallangan axborot tizimi;

antivirus dasturi – kompyuter virusiga qarshi dastur, viruslarni aniqlash uchun mo‘ljallangan va ularni yo‘q qilish taklifini berishi mumkin bo‘lgan yoki yo‘q qiluvchi dastur;

antivirus himoyasi – antivirus dasturlari yordamida kompyuter viruslari ta’sirining oldini olish, viruslarni topish va zararsizlantirishga qaratilgan chora-tadbirlar majmui;

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

axborot aktivlari – bank faoliyati uchun muhim bo‘lgan axborotlar (mijoz ma’lumotlari, operatsion ma’lumotlar, dasturiy ta’minot, ma’lumotlar bazalari, hodisalar jurnallari va boshqalar) hamda ularni saqlash, uzatish, qayta ishlash va muhofaza qilishga xizmat qiluvchi barcha resurslar (axborot tizimlari va resurslari, serverlar, ma’lumotlar omborlari, aloqa kanallari va dasturiy ilovalar);

axborot resursi – axborot tizimi tarkibidagi elektron shakldagi axborot, ma’lumotlar banki, ma’lumotlar bazasi, shu jumladan axborot tizimlarida ochiq shaklda joylashtiriladigan yoxud e’lon qilinadigan audio, video, grafik va matnli axborot;

axborot tizimi – axborotni to‘plash, saqlash, izlash, unga ishlov berish hamda undan foydalanish imkonini beradigan, tashkiliy jihatdan tartibga solingan jami axborot resurslari, axborot texnologiyalari va aloqa vositalari;

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

axborot xavfsizligi noxush hodisasi – axborot xavfsizligining yagona voqeasi yoki bir qator noxush yoxud kutilmagan voqealari bo‘lib, ushbu voqealar tufayli axborotning oshkor bo‘lishi va axborot xavfsizligiga tahdidlar ehtimoli;

hujum – axborot aktivlarini yo‘q qilish, ochish, o‘zgartirish, blokirovkalash, tutib olish, ruxsat etilmagan foydalanish huquqini olish yoki axborot aktivlaridan ruxsatsiz foydalanishga urinish;

kompyuter virusi – destruktiv xususiyatga, o‘z nusxasini ko‘paytira olish (asl nusxa bilan to‘liq mos bo‘lmasligi ham mumkin) va foydalanuvchi bilmagan holda ularni kompyuter tizimlari, tarmoqlari turli resurslari va shu borada joriy etish qobiliyatiga ega bo‘lgan dasturdir (bajariladigan kodlar to‘plami);

monitoring — avtomatlashtirilgan bank tizimi va axborot tizimlari holatini kuzatish;

server xonasi – bank serverlari, telekommunikatsiya qurilmalari, uzluksiz quvvat manbalari va boshqa hisoblash texnikalari joylashgan xona;

tarmoqlararo ekran – tizimga kelib tushadigan va (yoki) tizimdan chiqib ketadigan axborotning nazorat qilinishini amalga oshiradigan dastur va (yoki) dasturiy vosita;

xesh summasi – kriptografik algoritm yordamida hisoblangan, fayl butligini tekshirish summasi;

shaxsga doir ma’lumotlar – muayyan jismoniy shaxsga taalluqli bo‘lgan yoki uni identifikatsiya qilish imkonini beradigan, elektron tarzda, qog‘ozda va (yoki) boshqa moddiy jismda qayd etilgan axborot;

elektron arxiv – arxiv maqomiga ega bo‘lgan, bank elektron hujjatlarini jamlovchi, hisobga oluvchi, saqlovchi va foydalanishni amalga oshiruvchi bankning tarkibiy bo‘limi;

elektron hujjat – elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot;

oxirgi nuqtalar (Endpoint) – tarmoq tizimiga ulanadigan fizik uskunalardir. Bunda, mobil qurilmalar, kompyuterlar, virtual mashinalar, o‘rnatilgan uskunalar yoki serverlar oxirgi nuqtalar bo‘lishi mumkin;

kiberxavfsizlik tavakkalchiligi – axborot tizimlari, axborot-kommunikatsiya texnologiyalari infratuzilmasi yoki raqamli xizmatlariga qarshi yo‘naltirilgan tahdidlar natijasida yuzaga kelishi mumkin bo‘lgan moliyaviy zarar, operatsion faoliyatning izdan chiqishi yoki tashkilot obro‘siga putur yetishi ehtimoli;

DLP (Data Loss Prevention) – ma’lumotlarni ruxsatsiz tarqalishidan himoyalash tizimi;

PAM (Privileged Access Management) – axborot tizimlariga imtiyozli kirish huquqlariga ega bo‘lgan foydalanuvchilarni tizimga kirishini boshqarish, nazorat qilish va himoya qilish tizimi;

IDS/IPS (Intrusion Detection/Prevention System) – tajovuzlarni aniqlash va oldini olish tizimlari;

Wi-Fi (Wireless Fidelity) – ma’lumotlarni simsiz uzatish texnologiyasi;

VPN (Virtual Private Network) – virtual shaxsiy tarmoq.

2. Banklar axborot tizimlari va axborot resurslarida axborot xavfsizligi va kiberxavfsizlikni ta’minlashi hamda butun ish faoliyati davomida saqlab turishi lozim.

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

3. Banklar va ularning filiallarida (filiallar, amaliyot boshqarmalari, bank xizmatlari ofislari (markazlari) va boshqa alohida bo‘linmalar) axborot xavfsizligi va kiberxavfsizlikni ta’minlash maqsadida axborot xavfsizligi va kiberxavfsizlikni ta’minlash xizmati (bundan buyon matnda Xizmat deb yuritiladi) tashkil etiladi.

4. Xizmat bankning axborot aktivlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash, shuningdek tizimning vaqtincha to‘xtashi, to‘lov ma’lumotlarining noqonuniy o‘zgarishi, bank yoki uning mijoziga zarar yetkazish holatlarini oldini olish va bartaraf etish bo‘yicha mas’ul hisoblanadi.

5. Xizmat o‘z faoliyatida:

axborot xavfsizligi va kiberxavfsizlikni boshqarish tizimini tashkil qilishi, axborot xavfsizligi va kiberxavfsizlikni ta’minlash talablarining bank bo‘linmalari hamda xodimlari tomonidan bajarilishini tashkillashtirishi va nazorat qilishi;

axborotning saqlanishini ta’minlash ustidan nazoratni tashkil etishi;

axborotni muhofaza qilish masalalarida bank bo‘linmalari va xodimlariga uslubiy va amaliy yordam ko‘rsatishi;

axborot aktivlarida axborotni muhofaza qilish tizimini loyihalash, sinovdan o‘tkazish, qabul qilish va amaliyotda qo‘llash jarayonlarida ishtirok etishi, ushbu jarayonlarda bank siriga oid va boshqa konfidensial ma’lumotlar chetga chiqishining oldini olish choralarini ko‘rishi;

o‘z vakolati doirasida bankning axborot xavfsizligi va kiberxavfsizligini boshqarish, ta’minlash va nazorat qilish usullari, vositalari va mexanizmlarini tanlash, joriy etish va qo‘llashni amalga oshirishi;

axborot aktivlarida axborotdan ruxsatsiz foydalanishga urinishlar bo‘lganligi, unga boshqacha shaklda aralashilganligi aniqlanganda hamda tizimning ishlash qoidalari buzilganda mazkur tizimdagi axborotni muhofaza qilish chora-tadbirlarini ko‘rishi;

axborot aktivlariga nisbatan amalga oshiriladigan kibertahdidlar va hujumlarni aniqlashi, tahlil qilishi hamda ularni bartaraf etish choralarini ko‘rishi;

axborot xavfsizligi noxush hodisasi (bundan buyon matnda noxush hodisa deb yuritiladi) to‘g‘risidagi ma’lumotlarni yig‘ishi, qayta ishlashi, tahlil qilishi va saqlashi;

noxush hodisalarni tekshirish bo‘yicha ishlarni amalga oshirishi;

axborotni muhofaza qilish chora-tadbirlarining holati va samaradorligini tahlil qilishi;

axborot xavfsizligi va kiberxavfsizlikni ta’minlash dasturiy ta’minotlari va apparat-dasturiy qurilmalarining to‘g‘ri ishlashini nazorat qilishi va ta’minlashi;

axborot xavfsizligi va kiberxavfsizlikni ta’minlash bilan bog‘liq monitoringni olib borishi;

axborot xavfsizligi va kiberxavfsizlikni ta’minlash masalalari bo‘yicha takliflar tayyorlashi;

axborot aktivlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash choralarini ko‘rish uchun talablarni belgilashi;

bankning axborot aktivlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda nazorat qilish bo‘yicha rejalarni tuzishi;

konfidensial, shu jumladan bank sirini tashkil etuvchi va shaxsga doir ma’lumotlarning saqlanishini nazorat qilishi;

axborot tizimlarida to‘xtash, avariya holatlari, kiberxavfsizlik hodisasi hamda noxush hodisa sodir bo‘lganda tizimlarni qayta tiklash jarayonida ishtirok etishi va axborot tizimlarining to‘liq ishchi holatiga kelishini nazorat qilishi;

bank hujjatlariga muvofiq boshqa funksiyalarni amalga oshirishi kerak.

6. Xizmatning vazifalari, vakolatlari va majburiyatlari bankning ichki hujjatlari bilan belgilanishi mumkin, bunda mazkur Nizom talablari inobatga olinadi. Xizmat o‘zining vazifa va majburiyatlarini bajarishga zarur bo‘lgan texnik resurslar bilan ta’minlanishi lozim.

7. Xizmat xodimlarining soni ularga yuklatilgan vazifalar, axborot resurslari va axborot tizimlari soni hamda axborot xavfsizligi va kiberxavfsizlikni ta’minlash

tizimlarining avtomatlashtirilganlik darajasidan kelib chiqib belgilanadi.

8. Xizmat hamda axborot texnologiyalari bo‘linmalari bank boshqaruvi organining turli a’zolariga bo‘ysunishi lozim, bunda Xizmat to‘g‘ridan to‘g‘ri bank boshqaruvi raisiga bo‘ysunadi.

Xizmat xodimlarini ularning asosiy faoliyati bilan bog‘liq bo‘lmagan ishlarga jalb etish taqiqlanadi.

9. Banklar tizimli ravishda har yili kamida ikki marotaba axborot xavfsizligi va kiberxavfsizlikni ta’minlash sohasiga ixtisoslashtirilgan o‘quv kurslarida Xizmat xodimlarining malakasini oshirishni ta’minlashi kerak. Bunda Xizmatning barcha mas’ul xodimlarini yo‘nalishi bo‘yicha o‘qitish va malakasini oshirish inobatga olinishi lozim.

10. Axborot xavfsizligi va kiberxavfsizlikni ta’minlash qonunchilik hujjatlarida belgilangan talablar hamda bankning axborot xavfsizligi va kiberxavfsizlikni ta’minlashga oid ichki hujjatlari bilan tartibga solinadi.

11. Bank axborot xavfsizligiga oid ichki siyosatni ishlab chiqishi va qabul qilishi lozim.

Axborot xavfsizligi siyosatida bankda mavjud bo‘lgan barcha axborot tizimlari va axborot resurslarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha talablar belgilanadi.

12. Axborot xavfsizligi va kiberxavfsizlikni ta’minlashga oid ichki hujjatlar va ularda belgilangan talablar bankning har bir xodimiga tanishtirilishi shart. Bank xodimlari ushbu hujjatlarda belgilangan talablarga qat’iy rioya qilishlari kerak.

13. Axborot tizimlari va axborot resurslarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash bilan bog‘liq mazkur Nizomda belgilangan barcha chora-tadbirlar amalga oshirilganligi yozma yoki elektron shaklda o‘z tasdig‘iga ega bo‘lishi lozim.

14. Agar bank filiallar tarmog‘iga ega bo‘lsa, har bir filialda bankning tasdiqlangan axborot xavfsizligi va kiberxavfsizlikni ta’minlashga oid hujjatlari to‘plami mavjud bo‘lishi kerak. Muayyan filiallarning xususiyatlarini hisobga olish

zarur bo‘lsa, bank ushbu xususiyatlarni inobatga olgan holda o‘z ichki hujjatlarini ishlab chiqilishini ta’minlaydi.

15. Bankning axborot aktivlariga dasturiy o‘zgartirish kiritish yoki yangi axborot resurslari va tizimlarini joriy etish Xizmat bilan kelishilgan holda amalga oshirilishi lozim.

16. Banklarga o‘zlarining axborot-kommunikatsiya texnologiyalari infratuzilmalari hamda axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimlarini boshqarish, nazorat qilish va uzluksiz ishlashini ta’minlash vazifalarini shartnoma asosida xizmat ko‘rsatuvchi tadbirkorlik subyektlariga (autsorsing) berish taqiqlanadi.

3-bob. Konfidensial ma’lumotlarning oshkor etilishidan himoyalash

17. Bank qonunchilik hujjatlari va o‘zining ichki hujjatlari bilan belgilangan konfidensial ma’lumotlarning oshkor etilmasligini ta’minlaydi. Bunda, bank tomonidan quyidagilar bajarilishi lozim:

bankka yoki uning bo‘linmasiga taalluqli bo‘lgan konfidensial ma’lumotlar, shu jumladan bank sirini tashkil etuvchi va shaxsga doir ma’lumotlar ro‘yxatini belgilash va uning aktualligini ta’minlash;

yetkazilgan zararni qoplash maqsadida har bir xodim bilan konfidensial ma’lumotlarni sir saqlash bo‘yicha majburiyatnomani imzolash;

konfidensial ma’lumotlardan foydalanishga ruxsati mavjud bo‘lmagan xodimlarning ushbu ma’lumotdan foydalanmasligini ta’minlash;

konfidensial ma’lumotlarni o‘zida saqlovchi kompyuterlar va ulardagi hujjatlarning ishonchli saqlanishini ta’minlash;

O‘zbekiston Respublikasining “Bank siri to‘g‘risida”gi va “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonunlarida ko‘rsatilgan talablar bajarilishini ta’minlash;

konfidensial ma’lumotlardan ruxsatsiz foydalanishning oldini olish bo‘yicha choralar ko‘rish.

18. Telekommunikatsiya tarmog‘i orqali davlat sirlarini tashkil etuvchi ma’lumotlarning uzatilishi taqiqlanadi.

4-bob. Axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimini tashkil etish hamda axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini boshqarish

19. Bankda huquqiy, tashkiliy, texnik choralar va axborot muhofazasi tizimlari (qurilmalari) yig‘indilaridan iborat bo‘lgan axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimi tashkil etiladi.

20. Axborot xavfsizligi va kiberxavfsizlikni ta’minlashda foydalaniladigan dasturiy-texnik vositalar axborot xavfsizligi va kiberxavfsizlik talablariga muvofiq litsenziyalangan va sertifikatlangan bo‘lishi lozim. Bunda barcha dasturiy ta’minotlarni texnik qo‘llab-quvvatlash bo‘yicha amalga oshiriladigan ishlar dasturiy ta’minotning egasi yoki yetkazib beruvchi tomonidan ta’minlanishi shart.

21. Axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimi quyidagilarni:

axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini aniqlash, oldini olish va bartaraf etishni;

barcha axborot tizimlari va axborot resurslarining axborot muhofazasini ta’minlashni;

xalqaro standartlar asosida tajribadan o‘tgan eng ilg‘or yechimlarni qo‘llashni;

yuqori ishonchga ega bo‘lgan, xizmat ko‘rsatilishi oson bo‘lgan tizim, qurilma va uskunalarni qo‘llashni;

barcha jarayon va qurilmalardagi axborotlar bo‘yicha ma’lumotlarni qayd etib borishni, axborot xavfsizligining buzilishi, dastur, qurilma va foydalanuvchilarning ishlaridagi o‘zgarishlarni aniqlashni;

ish jarayonining soddaligini ta’minlashni va maksimal darajada harakatlarni avtomatlashtirishni;

muhofaza to‘siqlarini bir necha pog‘onalarda tashkil etishni;

axborot xavfsizligi va kiberxavfsizlikning uzluksizligini ta’minlashni;

noxush hodisalarni oldini olish va yuzaga kelganda ularni bartaraf etish hamda axborot tizimlarning ish faoliyatini qayta tiklashni;

axborot xavfsizligi va kiberxavfsizlikni doimiy mukammallashtirib borishni ta’minlaydi.

22. Axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimi quyidagilarni amalga oshiradi:

axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimlariga kirishni nazorat qilish;

tarmoq xavfsizligini ta’minlash;

axborot tizimlariga kirishni boshqarish va nazorat qilish;

zarar keltiruvchi dasturlardan (kompyuter viruslari va boshqalardan) muhofaza qilish;

muhofaza qilinayotgan ma’lumotlar va dasturlarni nazorat qilish, qayta tiklash, butligini aniqlash va monitoringini yuritish;

ma’lumotlarni qayta ishlash, saqlash va uzatilishida muhofazasini ta’minlash;

veb-resurslar, ma’lumotlar bazasi, ma’lumotlarni saqlash omborlari va boshqa axborot resurslarini turli axborot xavfsizligi xatarlaridan saqlash;

axborot muhofazasining ta’minlanganlik darajasini tekshirish, tahlil qilish va baholash;

elektron raqamli imzo kalitlari va sertifikatlarini taqsimlash, hisobini yuritish va boshqarish;

ma’lumotlarning uchinchi shaxslarga oshkor bo‘lishini oldini olish;

axborot tizimida axborot xavfsizligi va kiberxavfsizlik sozlamalari hamda axborot tizimining butligi bilan bog‘liq barcha o‘zgarishlarni nazorat qilish va elektron qayd yozuvlarini yuritish.

23. Banklar tizimlardagi xatoliklar va tashqi salbiy ta’sirlar natijasida yuzaga kelishi mumkin bo‘lgan axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini boshqarish tizimini yaratishi kerak.

24. Axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini boshqarish tizimi quyidagi funksiyalarni o‘z ichiga olishi kerak:

axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini aniqlash, yig‘ish, ro‘yxatga olish, baholash, kamaytirish choralarini ko‘rish, monitoring va nazorat qilish;

axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini bartaraf etish ishlarini rejalashtirish va boshqarish;

axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini boshqarish bo‘yicha hisobotni shakllantirish;

axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini qayta ko‘rib chiqish.

25. Xizmat axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimining nazoratini olib boradi va uzluksiz ishlashini ta’minlaydi.

Xizmat tomonidan bankda axborot xavfsizligi va kiberxavfsizlikni ta’minlash yuzasidan ma’lum bo‘lgan tavakkalchilik va qo‘llaniladigan boshqarish vositalari va usullarining ro‘yxati tuzilishi hamda bank boshqaruvi raisi tomonidan tasdiqlanishi lozim.

Bank axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklari ro‘yxatining dolzarbligini ta’minlashi kerak.

26. Axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini doimiy ravishda baholash va tahlil qilib borish Xizmat tomonidan amalga oshiriladi.

Xizmat bank boshqaruvi raisiga tavakkalchiliklarni ortishi bo‘yicha tegishli ma’lumotlarni taqdim etib borishi lozim.

27. Axborot xavfsizligi va kiberxavfsizlik tavakkalchiliklarini boshqarish bo‘yicha amalga oshirilgan chora-tadbirlar hujjatlashtirilishi va yiliga kamida bir

marotaba bank boshqaruvi raisi tomonidan ko‘rib chiqilib, tavakkalchiliklarni kamaytirish yuzasidan tegishli chora-tadbirlar o‘tkazilishi kerak.

28. Banklar faoliyatida axborot xavfsizligi va kiberxavfsizlikning ta’minlanganlik darajasini baholash bo‘yicha reyting axborot tizimi O‘zbekiston Respublikasi Markaziy banki (bundan buyon matnda Markaziy bank deb yuritiladi) tomonidan yuritiladi.

Reyting axborot tizimiga banklar tomonidan o‘z vaqtida va to‘g‘ri (haqqoniy) ma’lumotlar kiritilishi lozim.

5-bob. Noxush hodisalar va kiberxavfsizlik hodisalarini oldini olish hamda bartaraf etish

29. Banklarda axborot xavfsizligi siyosatining buzilishi quyidagilarga olib keladi:

axborot konfidensialligining buzilishi;

axborot butligining buzilishi;

texnologik jarayonning buzilishi;

axborotdan erkin foydalanish huquqining buzilishi.

30. Bankda noxush hodisalar to‘g‘risidagi ma’lumotlarni olish uchun monitoring tizimlari joriy etiladi. Bunda ushbu tizimlarning ishlashini monitoring qilish va yuzaga kelgan noxush hodisalarni bartaraf etish bo‘yicha doimiy ravishda ishlaydigan ishchi guruh tuziladi.

31. Noxush hodisalarni bartaraf etish uchun tashqi ekspertlar yoki texnik xizmat ko‘rsatuvchi tashkilot mutaxassislari jalb qilinishi mumkin. Noxush hodisalarni bartaraf qilish uchun tashqi ekspertlar yoki texnik xizmat ko‘rsatuvchi tashkilot mutaxassislari jalb qilinganda, bank ular bilan konfidensial ma’lumotlarni oshkor qilmaslik to‘g‘risida shartnoma tuzishi lozim.

32. Aniqlangan noxush hodisalar to‘g‘risidagi ma’lumotlar Xizmat tomonidan hujjatlashtirib borilishi lozim.

Xizmat noxush hodisa aniqlangan vaziyatda axborot xavfsizligi monitoringi tizimi ma’lumotlaridan foydalanishi va noxush hodisa ro‘y bergan vaqtdagi axborot tizimlarining elektron jurnallari va noxush hodisa sodir bo‘lgan tizim serverlarining shu vaqtdagi zaxira nusxalarini (backup, snapshot va boshqalar) saqlashi va ularning butligini ta’minlashi kerak.

33. Banklar texnik vositalardan foydalanganda noxush hodisalarni oldini olish maqsadida quyidagilarni ta’minlashlari zarur:

texnik vositalardan ruxsatsiz foydalanishni taqiqlash;

texnik vositalarni ruxsatsiz o‘chirib qo‘yilishidan himoya qilish;

monitoring va noxush hodisalarning elektron bayonnomalarini elektron arxivda saqlash va ruxsatsiz o‘zgartirish yoki yo‘q qilishdan himoyalash;

axborot tizimlari va resurslarini qonunchilikda belgilangan tartibda kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish.

34. Ish jarayonida noxush hodisalar aniqlanganda, bank xodimlari zudlik bilan bu haqda Xizmatni xabardor qilishlari kerak.

Noxush hodisalar sodir etilgan vaqtda Xizmat tomonidan amalga oshiriladigan harakatlar bankning ichki hujjatlarida belgilanadi.

35. Bank sodir bo‘lgan noxush hodisa to‘g‘risida Markaziy bank va vakolatli davlat organiga zudlik bilan yozma yoki elektron shaklda xabar berishi lozim.

6-bob. Axborot tizimlari va resurslarini monitoring qilish

36. Banklar konfidensial ma’lumotlar va barcha axborot aktivlaridan foydalanish monitoringini amalga oshiradi. Bunda monitoring qilishda quyidagilar belgilanadi:

axborot infratuzilmasining axborotga ishlov berish, 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 SIEM (Security Information and Event Management) yoki boshqa tizimlarni joriy qilish;

axborot xavfsizligi va kiberxavfsizlik hodisalari to‘g‘risidagi ma’lumotlarni to‘plash, tahlil qilish va ularga javob berish jarayonlarini avtomatlashtirish imkonini beruvchi SOAR (Security Orchestration, Automation and Response) tizimlarni joriy qilish;

axborot xavfsizligi va kiberxavfsizlikning ta’minlanganlik holatini monitoring qilish tizimi 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 kiberxavfsizlikni ta’minlashdagi cheklanishlar va boshqa hodisalar) bartaraf etish va (yoki) ularni oldini olish bo‘yicha choralar ko‘rish;

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

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

7-bob. Axborot tizimlari va resurslariga kirishni boshqarish

37. Banklar axborot tizimlari va resurslariga kirish va ushbu tizimlarda foydalanuvchilarning ishlash tartibini ishlab chiqishi kerak. Bunda yangi foydalanuvchilarning axborot tizimlari va resurslariga kirish hamda ushbu tizimlarga kirish huquqi bekor bo‘lgan foydalanuvchilarni undan chiqarish qoidalari inobatga olinishi lozim.

38. Yangi foydalanuvchilar axborot tizimlari va resurslariga Xizmat tomonidan kerakli texnik choralar ko‘rilib, ruxsat berilganidan keyin kiritiladi.

39. Xizmat axborot tizimlari va resurslariga kirishga ruxsat berilgan foydalanuvchilar ro‘yxatini hamda ularning ushbu tizimlardan foydalanishi bankda o‘rnatilgan tartibga muvofiqligini nazorat qiladi.

40. Banklar markazlashgan holda quyidagilarni ta’minlashi zarur:

axborot tizimlarida ishga yangi qabul qilingan xodimlar uchun hisobga olish yozuvlarini avtomatik tarzda yaratish;

xodimlarga ularning lavozim majburiyatlaridan kelib chiqib tegishli axborot tizimlariga kirish huquqlarini berish;

xodimlar axborot tizimlariga masofadan himoyalangan aloqa kanallari orqali, axborot xavfsizligi va kiberxavfsizlikni ta’minlash talablariga rioya qilgan holda, faqatgina O‘zbekiston Respublikasi hududida kirishini ta’minlash;

xodim boshqa lavozimga o‘tganida, mehnat ta’tiliga chiqqanida yoki ishdan bo‘shaganida uning hisobga olish yozuvlarini (akkauntlarini) o‘zgartirish, bloklash va cheklash.

41. Bank xodimlarga axborot tizimlari va resurslaridan foydalanish huquqini ularning funksional vazifalariga muvofiq holda beradi. Bunda, Xizmat quyidagilarni ta’minlashi lozim:

bankning axborot tizimlari va resurslaridagi xodimlarning hisobga olish yozuvining (akkaunt) butun hayot davrini boshqarish, uzluksiz nazorat qilish, shuningdek kadrlar tizimidagi ma’lumotlarga asoslanib, xodimlarning lavozim majburiyatlari va vakolatlarini doimiy ravishda tekshirib turish;

bankning tashkiliy tuzilmasi asosida rollarga asoslangan kirish modelini boshqarish va nazorat qilish, shuningdek xodimning atributlari va holatiga asoslangan holda axborot resurslarini (ular bilan bog‘liq hisob yozuvlari, kirish huquqlari va axborot tizimlaridagi vakolatlar) dinamik tarzda tayinlashni ta’minlash;

xodimning biznes roli yoki vazifasi o‘zgarganda, markazlashtirilgan tizim orqali yangi rolga mos ravishda kirish huquqlari va vakolatlarini avtomatik tarzda berish;

har bir axborot tizimi foydalanuvchilarining amaliy kirish huquqlari va vakolatlarini nazorat qilish hamda kelishilgan kirish huquqlari o‘rtasidagi farqlarni aniqlash;

bankning har qanday axborot tizimlari va resurslariga kirish huquqlari va vakolatlarni (to‘g‘ridan to‘g‘ri tayinlash, rol modeli bo‘yicha tayinlash, so‘rov

orqali tayinlash) paydo bo‘lish manbasini kuzatib borish hamda vakolatning paydo bo‘lish manbasi va zanjiri haqida to‘liq ma’lumotga ega bo‘lish.

42. Xizmat bank xodimlariga berilgan ortiqcha huquqlarni aniqlash vositalari bilan ta’minlanishi lozim.

43. Bank tomonidan axborot aktivlaridan foydalanishda foydalanuvchi amalga oshirgan operatsiya to‘g‘risidagi quyidagi ma’lumotlar:

bajarilgan operatsiya sanasi (kun, oy, yil) va vaqti (soat, daqiqa, soniya);

foydalanuvchiga tizimlarda hamda axborot dasturlarida berilgan foydalanuvchi identifikatori;

foydalanuvchi qurilmasining identifikatsiya ma’lumotlari (IP-manzil, MAC-manzil, qurilmaning nomi va boshqa identifikatorlari);

foydalanuvchining tizimdagi faol sessiyasi davrida bajargan barcha amaliyotlari va harakatlari tegishli elektron bayonnomalarda qayd etib borilishi lozim. Bunda, elektron bayonnomalardagi yozuvlarni o‘zgartirish yoki o‘chirish imkoniyati faqatgina bank boshqaruv raisining buyrug‘i bilan yuklatilgan Xizmat xodimlarida bo‘lishi shart.

44. Xizmat bank xodimlarining lavozim majburiyatlari, vakolatlari va axborot aktivlariga kirish huquqlarini bir oyda kamida bir marotaba tekshirib turishi hamda tekshiruv natijalarini hujjatlashtirib borishi lozim.

45. Xizmat bankning axborot tizimlari va resurslaridan ruxsatsiz foydalanishni oldini olish maqsadida:

foydalanuvchilarni identifikatsiya va autentifikatsiya qilishi hamda ushbu jarayonni boshqarishi;

muvaffaqiyatsiz kirishga urinishlarni aniqlashi va ularni cheklashi hamda ushbu foydalanuvchining axborot tizimlari va resurslariga kirish huquqini (akkauntini) bloklashi;

foydalanuvchining uzoq vaqt oralig‘ida harakatsizligi aniqlanganda ish sessiyasini to‘xtatishi;

axborot aktivlari hamda ishchi stansiyalarda foydalanuvchining ishlash davrida foydalanuvchi akkauntining bir vaqtning o‘zida bir nechta qurilmalarda ishlashini (multisessiya) cheklashi;

foydalanuvchining axborot aktivlarida shu axborot aktivlarining faoliyatiga ta’sir etadigan sozlamalarini (parametrlarini) o‘zgartirish imkoniyatini cheklashi;

muhim axborot infratuzilmasi obyekti sifatida, qonunchilikda belgilangan tartibda bankning axborot tizimlari hamda resurslarida axborot xavfsizligi va kiberxavfsizlikning ta’minlanganlik holati bo‘yicha baholash ishlari o‘tkazilishini ta’minlashi;

axborot tizimlari va resurslarini kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish hamda kiberxavfsizlikning ta’minlanganlik holatini baholash jarayonlarida aniqlangan kamchilik va zaifliklarni zudlik bilan bartaraf etishi lozim.

46. Axborot tizimlarida to‘lovlarga oid ma’lumotlarni kiritish, o‘zgartirish, tasdiqlash va o‘chirish huquqiga ega bo‘lgan foydalanuvchilarni autentifikatsiya qilish apparat-dasturiy qurilmalar orqali amalga oshiriladi.

Har bir foydalanuvchi tizimga kirish uchun uning o‘ziga ajratilgan apparat-dasturiy qurilmadan foydalanishi lozim.

47. Masofadan turib bank xizmatlarini ko‘rsatishning barcha jarayonlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash choralari bankning ichki hujjatlarida belgilanadi.

Masofadan turib bank xizmatlarini ko‘rsatish tizimida foydalanuvchilarning tizimga kirishi, axborot almashinuvi va ularning amallari to‘g‘risidagi to‘liq ma’lumotlar (IP va (yoki) MAC manzili, mobil telefondan foydalanganda – IMEI-kod) elektron bayonnomalarda qayd etib borilishi kerak.

Banklar barcha tizim foydalanuvchilariga ruxsat berilgan vaqtdan tashqari holatda bank tizimiga ulanishini taqiqlashi lozim. Bunda, bank tizimi bilan bog‘lanuvchi faol sessiyalar uzilishi shart.

48. Bankning axborot-kommunikatsiya texnologiyalari infratuzilmalari, axborot tizimlari va resurslari hamda axborot xavfsizligi va kiberxavfsizlikni

ta’minlash tizimlari administratorlarining barcha harakati PAM tizimi orqali amalga oshirilishi shart. Bunda foydalanuvchilarning harakatlarini ushbu tizim orqali qayd etish va imtiyozli sessiyalarini audit qilish talab etiladi.

49. Banklar PAM tizimida foydalanuvchilarning harakati qayd etilgan ma’lumotlarni kamida olti oy davomida saqlanishini ta’minlashi lozim.

8-bob. Ma’lumotlar bazasini boshqarish tizimi

50. Banklar ma’lumotlar bazasi sozlanishlarida xatoliklarni oldini olishi va tajovuzkorning quyidagi harakatlarini cheklashlari kerak:

ma’lumotlar bazasiga kirish;

ma’lumotlar bazasining maxsus interfeysini qo‘llash, komandalar kiritish va dasturlarni ishlatish;

administrator va foydalanuvchilar parollarini bilib olish;

ma’lumotlar bazasining tizim fayllariga kirish;

zararli dasturlar o‘rnatish;

serverning ilova dasturlariga egalik qilish;

ma’lumotlar bazasi va serverga masofadan hujum qilish.

51. Banklar ma’lumotlar bazasiga kiritiladigan barcha dasturiy o‘zgartirishlarni hujjatlashtirishi va kiritilgan o‘zgartirishlarning hisobini yuritishi lozim.

Ishchi stansiyalar va boshqa hisoblash texnikalarining operatsion tizimi, antivirus dasturi va boshqa dasturiy o‘zgartirishlar test-sinov ishlari yakuniga ko‘ra ishga tushiriladi. Ma’lumotlar bazasiga kiritiladigan barcha dasturiy o‘zgartirishlar avval test-sinov serverida tekshirilishi hamda ijobiy natijaga erishilganda ishchi serverga joriy etilishi lozim.

52. Ma’lumotlar bazasida o‘rnatilgan serverning ish jarayoni uchun zarur bo‘lmagan xizmatlar to‘xtatilishi va axborot portlari yopib qo‘yilishi lozim.

Ishlatiladigan axborot portlarining ro‘yxati foydalanish maqsadi ko‘rsatilgan holda bank boshqaruvi raisi tomonidan tasdiqlanadi.

53. Bankda real vaqt rejimida shubhali harakatlarni tezkor aniqlash va oldini olish uchun ma’lumotlar bazasi faoliyatini monitoring qilish tizimi DAM (Database Activity Monitoring) joriy etilishi lozim.

54. Ma’lumotlar bazasining administratori va ma’lumotlar bazasida axborot xavfsizligini ta’minlovchi xodimlarning vazifalari, vakolatlari va javobgarliklari bankning ichki hujjatlari bilan belgilanadi.

55. Ma’lumotlar bazasi administratorining paroli 12 ta belgidan kam bo‘lmasligi lozim, bunda parolning belgilari sifatida pastki va yuqori registr harflari, raqamlar va maxsus belgilar (@,#, $, &, % va h.k.) qo‘llaniladi. Parollar va tokenlar ma’lumotlar bazasida shifrlangan holda saqlanishi lozim.

56. Bank ma’lumotlar bazasiga boshqa tashkilotlarni faqatgina veb-servis (API) orqali ulanishini ta’minlashi shart. Boshqa tashkilotlarni to‘g‘ridan to‘g‘ri ulash (DB Link) taqiqlanadi.

9-bob. Tarmoq xavfsizligi

57. Tarmoq xavfsizligini loyihalashtirish, joriy etish va boshqarish quyidagi standartlar asosida amalga oshiriladi:

O‘z DSt ISO/IEC 27033-1:2016 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 1-qism. Sharh va konsepsiyalar";

O‘z DSt ISO/IEC 27033-2:2016 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 2-qism. Tarmoq xavfsizligini loyihalashtirish va joriy etish bo‘yicha rahbariy ko‘rsatmalar";

O‘z DSt ISO/IEC 27033-4:2016 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 4-qism. Xavfsizlik shlyuzlarini qo‘llagan holda tarmoqlararo xavfsizligini ta’minlash uchun kommunikatsiyalar";

O‘z DSt ISO/IEC 27033-5:2016 "Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Tarmoq xavfsizligi. 5-qism. Virtual xususiy tarmoqlarni qo‘llagan holda tarmoqlararo xavfsizligini ta’minlash uchun kommunikatsiyalar".

58. Banklar tarmoq xavfsizligini ta’minlash uchun quyidagi shartlarni bajarishi kerak:

korporativ tarmoq va axborot tizimlarining o‘zaro bog‘lanishida telekommunikatsiya hamda tarmoq servislari uzluksiz ishlashi va xavfsizligini ta’minlash;

tarmoq qurilmalari va dasturiy ta’minotning sozlamalari va uning komponentlarini ruxsatsiz ko‘rish yoki o‘zgartirishni cheklash;

tarmoqlarni alohida segmentlarga bo‘lish;

kibertahdidlarni real vaqt rejimida monitoring va tahlil qilish hamda bloklash imkoniyatini ta’minlash;

tarmoqdagi faollik to‘g‘risidagi batafsil ma’lumotlarni yig‘ish va saqlash;

tuzoqlar (honeypot) yaratish va ularni emulyatsiya qilish imkoniyatini ta’minlash;

tarmoq trafigini turli protokol va dasturlar darajasida tahlil qilish imkoniyatini ta’minlash;

tarmoqlararo axborot almashinuvida ma’lumotlarning konfidensialligini ta’minlash va tarmoqda ruxsatsiz harakatlarni oldini olish.

59. Korporativ tarmoqqa faqat ruxsat berilgan qurilmalar (hisoblash texnikasi) ulanishiga ruxsat berilishi lozim.

Bankka tegishli bo‘lmagan kompyuter qurilmalarini bankning korporativ tarmog‘iga ulanishiga ruxsat berishda quyidagilar ta’minlanishi shart:

korporativ tarmoqqa Xizmat bilan kelishgan holda bank rahbariyati ruxsati bilan ulash;

ulanadigan qurilmaning texnik parametrlari va identifikatorlarini qayd etish;

ulanadigan qurilmada litsenziyalangan antivirus dasturining mavjudligiga ishonch hosil qilish;

ulanadigan qurilmaga ma’lumotlarni ruxsatsiz tarqalishidan himoyalash tizimini (DLP) o‘rnatish;

ulanadigan qurilmaga axborot-kommunikatsiya texnologiyalari infratuzilmalari hamda axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimlarida ishlashga ruxsat berilishi ko‘zda tutilgan bo‘lsa, uni PAM tizimi orqali ulash;

konfidensial ma’lumotlar bilan ishlash tartibi bilan tanishtirish va majburiyatnoma imzolatish;

korporativ tarmoqqa ulanuvchi qurilmalarda internet tarmog‘iga ulanishni oldini olish;

bankda axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha belgilangan qo‘shimcha choralarni ko‘rish.

60. Korporativ tarmoqda axborot almashinuvining elektron bayonnomasi yuritilishi va elektron bayonnomada tizimga kirgan foydalanuvchining nomi (user name), vaqti, IP va (yoki) qurilmaning MAC manzili qayd etib borilishi kerak.

61. Banklar tomonidan tashkil etilgan korporativ tarmoqning (Markaziy bank tarmog‘iga, Internet jahon axborot tarmog‘iga, telekommunikatsiya provayderlariga, filiallarga va boshqa tarmoqlarga bog‘lanish) chizmasi Markaziy bank bilan kelishiladi.

62. Korporativ tarmoq xavfsizligining to‘liq nazorati va monitoringi doimiy ravishda Xizmat tomonidan amalga oshiriladi.

63. Bankning tarmoqlararo axborot almashinuvi xususiy virtual tarmoqlarni (VPN) tashkil etish yo‘li bilan muhofazalanadi.

Korporativ tarmoqda ilova serverlari bilan foydalanuvchilar o‘rtasidagi o‘zaro axborot almashinuvida himoyalangan protokol qo‘llanilishi lozim.

64. Bankning lokal hisoblash tarmog‘iga boshqa tarmoqlardan va (yoki) tashqi aloqa kanallari orqali bog‘lanish nuqtalari tarmoqlararo ekran qurilmalari bilan muhofalanadi.

65. Telekommunikatsiya shkaflari qulflanishi va videokuzatuv tizimlari orqali nazoratga olingan bo‘lishi lozim.

Lokal hisoblash tarmoqlari kabellarini telekommunikatsiya shkaflari bilan hisoblash texnikalari, bankomat va boshqa qurilmalarning bog‘lanish nuqtalarigacha muhofazalanmagan tarzda o‘tkazilishi taqiqlanadi.

66. Bankning barcha bo‘linmalari lokal hisoblash tarmog‘ida virtual mahalliy tarmoqlar (VLAN) hosil qilish yo‘li bilan bir-biridan ajratilishi lozim.

67. Bankda tarmoq xavfsizligini ta’minlashda qo‘llaniladigan dasturiy ta’minot va texnik vositalarning holatlarini monitoring qilib borilishi, statistik ma’lumotlar yig‘ilishi va tahlil qilinishi, yuzaga kelayotgan muammolar ilk bosqichda aniqlanishi va ular asosida favqulodda vaziyatlar paydo bo‘lishining oldi olinishi lozim.

68. Banklar tarmoqdagi tahdidlarni aniqlash va ularga qarshi javob beruvchi tizimlarni NDR (Network Detection and Response) joriy qilishi lozim.

69. Banklar tajovuzlarni aniqlash va oldini olish tizimini (IDS/IPS) qo‘llashi lozim, ya’ni bank tarmoq ichida noodatiy harakatlarni va lokal hisoblash tarmoqlaridagi hujumlarni aniqlash, oldini olish va to‘sish uchun mo‘ljallangan dasturiy yoki dasturiy-apparat vositalarni joriy etishlari lozim.

Banklar real vaqt rejimida tarmoq dasturlari ishlashidagi og‘ishlar, shuningdek kompyuter tizimi yoki tarmoqda ruxsat etilmagan foydalanish (ruxsatsiz kirish yoki tarmoqqa hujumlar) holatlarini aniqlash imkoniyatiga ega bo‘lishi kerak. Bank IDS/IPS tizimlarining bazasini aktual holatda bo‘lishini ta’minlaydi.

IPS/IDS tizimlari tarmoq infratuzilmasining miqyosi serverlar va kommutatsiya uskunalari (marshrutizatorlar, kommutatorlar, aloqa liniyalari) interfeyslarining o‘tkazish qobiliyatidan kelib chiqib tanlanadi va joriy etiladi. Agar telekommunikatsiya qurilmalari ma’nan eskirgan bo‘lsa va IPS/IDS tizimlariga ishlash imkoniyatini bermasa, ushbu qurilmalar yangilanishi lozim.

70. Banklarda qo‘llaniladigan tarmoqlararo ekran qurilmalari O‘z DSt 2815:2014 “Axborot texnologiyalari. Tarmoqlararo ekran.” standarti talablarining

kamida ikkinchi toifasiga mos bo‘lishi kerak.

Tarmoqlararo ekran qurilmalarining sozlanishlari tasdiqlanishi va ruxsat berilgan axborot almashinuvi protokollari asoslangan bo‘lishi lozim. Sozlanishlarga kiritiladigan o‘zgartirishlar bank tomonidan amalga oshiriladi.

71. Asosiy va zaxira tarmoqlararo ekran qurilmalarining sozlamalari bir xil bo‘lishi hamda aktual holda elektron arxivda saqlanishi kerak.

72. Tarmoqlararo ekran qurilmalari va proksi-serverlarning elektron bayonnomalari Xizmat tomonidan tahlil qilib boriladi va tashqi hujumlar aniqlanganda zudlik bilan Markaziy bankka xabar beriladi.

10-bob. Elektron pochta va internet tarmog‘idan foydalanish

73. Bank o‘zining ichki elektron pochta tizimi serverini bankning lokal hisoblash tarmog‘ida yaratadi

Tezkor xabarlar almashish tizimlari (messenger) yoki dasturlaridan foydalanish, bank tomonidan internet tarmog‘idan va elektron pochta tizimlaridan foydalanishda axborot muhofazasini ta’minlash, xodimlarni tizimga kiritish, ularga cheklovlar qo‘yish, javobgarlik, xodimlar harakati va tizimning axborot xavfsizligi ustidan nazorat qilish bankning ichki hujjatlarida belgilanadi

74. Bank xodimlariga bank faoliyatiga tegishli bo‘lmagan ma’lumotlarni bankning elektron pochtasi orqali uzatish taqiqlanadi.

75. Bank bo‘limlari va filiallari o‘rtasida axborot almashinuvi elektron hujjat aylanishi dasturlari yoki bankning ichki elektron pochta tizimi orqali amalga oshiriladi.

76. Fayllarni uzatish protokolidan (FTP) foydalanib tashkil qilingan umumiy katalog (FTP Server) orqali fayl almashinuvini amalga oshirish va bank siri ma’lumotlarini tarmoqda erkin o‘qish uchun joylashtirish taqiqlanadi.

Elektron pochta orqali qabul qilinadigan va yuboriladigan ma’lumotlarda zararli kodlarning mavjudligini tekshirish tizimi (Sandbox) joriy etilishi lozim. Xizmat ushbu tizimni nazorat qilib boradi.

77. Bank o‘zining elektron pochta tizimi hamda internet tarmog‘idan foydalanish tartibini ichki hujjatlari bilan belgilaydi hamda elektron pochta orqali yuborilgan va qabul qilingan ma’lumotlarni Xizmat tomonidan nazorat qilinishini ta’minlaydi. Bunda, faqat ruxsat berilgan foydalanuvchilar internet tarmog‘idan foydalanishi mumkin.

78. Bankda internet tarmog‘idan foydalanishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash choralari ko‘rilishi kerak.

Konfidensial, jumladan bank sirini tashkil etuvchi va shaxsga doir ma’lumotlar bilan ishlaydigan foydalanuvchilarning kompyuterlarini internet tarmog‘iga proksi server orqali ulashga ruxsat etiladi. Bunda faqat ish faoliyatiga oid axborot resurslarining ro‘yxati asosida internet tarmog‘iga ulanishi tashkil etilishi lozim.

79. Avtomatlashtirilgan bank tizimi ma’lumotlar bazasi serverlari, dastur serverlari, to‘lov tizimi ma’lumotlarini qayta ishlovchi barcha serverlar hamda bankning ish faoliyatida qatnashuvchi boshqa muhim serverlari bankda tashkil etilgan alohida ajratilgan va muhofaza qilingan tarmoq segmentida joylashtirilishi lozim.

Bankning internet tarmog‘i orqali ulanadigan axborot tizimlari va resurslari hujumni aniqlash va uni oldini olish bo‘yicha IDS/IPS, WAF (Web Application Firewall) hamda Anti-DDoS tizimlari bilan muhofazalangan bo‘lishi kerak.

80. Axborot muhofazasini kuchaytirish maqsadida tarmoq protokolida tarmoq tranzit paketlarining IP manzillarini o‘zgartirish imkonini beruvchi tarmoq manzillarini o‘zgartirish protokoli (NAT) qo‘llanilganda, barcha ulanishlarning elektron jurnallari asl IP manzillar ko‘rsatilgan holda yuritilishi va belgilangan tartibda elektron arxivga olinishi lozim.

Internet tarmog‘idan foydalanish tartibi nazoratga olingan bo‘lishi va bank xodimlarining internet tarmog‘idan foydalanishlari ularning lavozim yo‘riqnomasiga ko‘ra belgilanishi lozim.

81. Internet tarmog‘idan foydalangan xodimning logini, foydalanish vaqti, resurs nomi va boshqa ma’lumotlar aks ettirilgan elektron bayonnomalar yuritilishi kerak. Xizmat ushbu elektron bayonnomalarni tahlil qilib boradi.

82. Internet tarmog‘idan foydalanishda axborot muhofazasini ta’minlash tarmoqlararo ekran qurilmalari, proksi-serverlar, antivirus vositalari, ruxsatsiz kirishni aniqlash va oldini olish (IDS/IPS) hamda boshqa axborot xavfsizligi va kiberxavfsizlikni ta’minlash tizimlarini qo‘llash yo‘li bilan amalga oshiriladi.

83. Bank tarmog‘i va kompyuterlarga modemlar yoki uyali telefonlarni ulash, shuningdek internet tarmog‘ida ishlashda tashqi proksi-serverlardan foydalanish va bankning ichki lokal tarmog‘ini simsiz tashkil etish va bank kompyuterlarida simsiz axborot almashinuvi tizimlaridan foydalanishga yo‘l qo‘yilmasligi ta’minlanishi kerak.

84. Mijozlar va bank iste’molchilari uchun qulayliklar yaratish maqsadida bank binosida Wi-Fi zonalari tashkil etilishi mumkin.

Bunda, Wi-Fi texnologiyasi bank ichki lokal tarmog‘idan jismonan ajratilgan bo‘lishi hamda unda quyidagi axborot xavfsizligi va kiberxavfsizlikni ta’minlash choralari ko‘rilgan bo‘lishi kerak:

Wi-Fi tarmog‘i orqali faqatgina internet tarmog‘iga kirishga ruxsat berish;

mijozni identifikatsiyadan o‘tkazish;

mijozlararo ulanishni taqiqlash (client isolation);

IPS/IDS yoki proksi filtrlash orqali shubhali va zararli trafikni bloklash;

DoS hujumlarini oldini olishda tezlik (QoS) va sessiyalarni cheklash;

Wi-Fi tarmog‘iga ulanish to‘g‘risidagi bayonnomalarni (MAC, IP, sana/vaqt, mexmon identifikatori) kamida olti oy davomida saqlash;

WPA2/WPA3-PSK yoki WPA2-Enterprisedan foydalanish va trafikni majburiy shifrlash;

himoyasiz ochiq parolli (shifrlanmagan) Wi-Fi tarmog‘idan foydalanishni taqiqlash;

real vaqt rejimida anomal faollik, skanerlash va hujumga urinishlar hamda taqiqlangan resurslarga ulanishni kuzatish;

Rogue AP, Spoofing va boshqa hujumlarni aniqlash va oldini olish tizimini (WIDS/WIPS) ishlatish.

85. Bank internet tarmog‘idagi tashqi axborot resurslarini muntazam ravishda kuzatib borishi shart. Bundan ko‘zlangan asosiy maqsad bankning ramziy belgisi, ishbilarmonlik obro‘si va boshqa elementlaridan noqonuniy foydalangan holda mijozlar va hamkorlarni chalg‘itishning oldini olish hisoblanadi. Bunda, bank bilan bog‘liq quyidagi holatlar aniqlanishi lozim:

bankning rasmiy veb-saytiga o‘xshatib yaratilgan soxta veb-saytlar (fishing nusxalar, soxta domenlar, sahifa nusxalari);

ijtimoiy tarmoqlar, messenjerlar, onlayn savdo maydonchalari, reklama platformalari va forumlardagi soxta akkauntlar;

rasmiy mobil ilovalar do‘konlaridagi (Google Play, App Store va boshqalar) soxta ilovalar;

bank nomidan yuborilgan fishing yoki firibgarlik xarakteridagi elektron pochta va SMS-xabarlar;

bankning tovar belgisi, ramziy belgisi (logo) yoki domeni nomidan noqonuniy foydalanish holatlari;

mijozning ishonchini yo‘qotish yoki ularni chalg‘itishga qaratilgan salbiy axborotlar (soxta ma’lumotlar, qalbakilashtirilgan yangiliklar, bank nomidan yozilgan sharhlar va hokazo);

bank nomidan noqonuniy foydalanish bilan bog‘liq boshqa holatlar.

Bank internet tarmog‘idagi tashqi axborot resurslarida yuqoridagi holatlarni aniqlagan taqdirda, bu haqda bir kun ichida Markaziy bank va O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi huzuridagi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat inspeksiyasiga xabar berishi hamda o‘zining rasmiy axborot manbalarida e’lon qilishi lozim.

11-bob. Texnik vositalarni boshqarish tizimi

86. Banklar axborot aktivlarida tarmoq obyektlari bo‘lgan foydalanuvchilar, kompyuterlar, serverlar va boshqa texnik vositalarni boshqarish (Active Directory

yoki boshqa muqobil) tizimini joriy etadi.

Bunda ushbu tizim yordamida kompyuterlarda foydalanuvchilar tomonidan faqat o‘zlarining ish faoliyatiga tegishli bo‘lgan dasturlar ishlatilishi va kompyuterlarga kirish himoyalanishi (parollar) ta’minlanadi.

Foydalanishga yo‘l qo‘yiladigan dasturlar ro‘yxati bank tomonidan belgilanadi. Ro‘yxatda bo‘lmagan barcha dasturlarni ishlatish va qo‘shimcha dasturlar o‘rnatish kabi harakatlar taqiqlanadi.

87. Texnik vositalarni boshqarish tizimi administrator tomonidan amalga oshiriladi, bunda Xizmat administratorning tizimdagi barcha harakatlarini nazorat qilishi kerak.

88. Xizmat kamida bir oyda bir marotaba texnik vositalarni boshqarish tizimining sozlamalari va elektron bayonnomalarini tahlil qilishi, texnik vositalardan foydalanishda bankning axborot xavfsizligiga oid siyosatida belgilangan talablarning bajarilishini nazorat qilishi kerak.

12-bob. Oxirgi nuqtalarda xavfsizlikni ta’minlash

89. Banklar axborot tizimlaridan ruxsatsiz ma’lumotlar uzatilishining oldini olish maqsadida ma’lumotlarni ruxsatsiz tarqalishidan himoyalash tizimini (DLP) joriy etishlari lozim.

Konfidensial ma’lumotlar bilan ishlash huquqi berilgan barcha oxirgi nuqtalar DLP tizimiga ulangan bo‘lishi lozim.

90. Ma’lumotlarni himoya qilishda banklar tomonidan:

muhofazalanadigan ma’lumotlarni ruxsatsiz turli tarmoq kanallari orqali uzatilishi, ruxsatsiz hisobga olinmagan tashqi tashuvchiga ko‘chirilishi, ruxsatsiz chop etilishi aniqlanishi hamda bu haqda bank rahbariyatiga ma’lumot berish va kelgusida shu kabi salbiy holatlar bo‘lmasligining oldini olish choralari ko‘rilishi;

muhofazalanadigan ma’lumotlarni server va kompyuterlarda saqlanishi nazorat qilinishi lozim.

91. Nazorat qilish tartib-qoidalari bankning ichki hujjatlari bilan belgilanadi va ma’lumotlarni ruxsatsiz tarqalishidan himoyalash Xizmat tomonidan amalga

oshiriladi.

92. Banklarda axborot xavfsizligi va kiberxavfsizlikni ta’minlash uchun antivirus himoyasi tashkil etilishi lozim.

93. Bankda antivirus dasturlarining o‘rnatilishi hamda ishlashi Xizmat tomonidan nazorat qilinadi.

94. Banklar kompyuter virusi aniqlanganda, ularning tarmoq orqali tarqalishini oldini olish maqsadida amalga oshiriladigan choralarni belgilashi kerak.

Bankning axborot infratuzilmasiga kompyuter virusi zarar keltirganligi aniqlanganda, banklar shu virusning kelib chiqishi va uning turi haqida Markaziy bankka ma’lumot berishi lozim.

95. Xizmat Bank xodimlari tomonidan ularning kompyuteridagi antivirus dasturining sozlamalarini o‘zgartirish imkoniyatini cheklashi kerak. Kompyuter virusi aniqlanganda, xodimlar tomonidan amalga oshiriladigan harakatlar banklar tomonidan belgilanishi hamda barcha xodimlarga tanishtirilishi lozim.

96. Banklar antivirus himoyasini tashkil etishda quyidagilarni ta’minlashi shart:

litsenziyaga ega antivirus dasturlaridan foydalanish va ularning litsenziyasining amal qilish muddati aktualligini ta’minlash;

antivirus dasturlarini markazlashgan holda boshqarish;

antivirus dasturlari bazalarini har kuni yangilab borilishini yo‘lga qo‘yish;

antivirus dasturining rusumi aktual (ma’nan eskirmagan) bo‘lishini ta’minlash;

barcha serverlar, kompyuterlar, bankomatlar, infokiosklar va boshqa antivirus dasturlari o‘rnatilishi mumkin bo‘lgan hisoblash vositalariga antivirus dasturlarini o‘rnatish.

97. Banklar axborot tizimlaridagi yangilanishlar va tuzatmalarni boshqarish tizimini joriy etishi lozim.

Zararli dasturlar va eksploitlardan himoyalanish maqsadida anomal faoliyatni kuzatish imkonini beruvchi EDR (Endpoint Detection and Response) texnologiyasidan foydalanilishi lozim.

Oxirgi nuqtalarda xavfsizlikni ta’minlash uchun Wi-Fi tarmoqlariga ulanishni taqiqlash lozim.

98. Bank tomonidan konfidensial ma’lumotlar bilan ishlash uchun berilgan mobil qurilmalar markazlashtirilgan holda boshqariladi va ularda xavfsizlik siyosatidan foydalaniladi (qurilmani masofadan bloklash, ma’lumotlarni masofadan o‘chirish va boshqalar).

99. Bank o‘zining axborot aktivlarida ruxsat etilmagan o‘zgarishlar haqida darhol ogohlantiruvchi va konfiguratsiya fayllarining yaxlitligini nazorat qilish tizimlaridan FIM (File Integrity Monitoring) foydalanishi shart.

13-bob. Elektron raqamli imzo va shifrlash kalitlaridan foydalanish

100. Banklarda elektron hujjatlarning asliga to‘g‘riligini tasdiqlash va tashqi muhit ta’siridan muhofazalash uchun bankning elektron raqamli imzo kalitlarini ro‘yxatga olish markazi tomonidan yaratilgan elektron raqamli imzo va shifrlash kalitlari qo‘llaniladi.

101. Banklar tashqi tizimlar bilan o‘zaro ishlashda bank tavakkalchiliklaridan kelib chiqqan holda elektron raqamli imzo va shifrlash kalitlarini qo‘llash bo‘yicha talablarni o‘zaro kelishgan holda amalga oshiradi.

102. Axborot aktivlari foydalanuvchilarining elektron raqamli imzo kalitlari maxsus yoki mobil qurilmalarga yozilgan bo‘lishi hamda har qanday usul bilan ruxsatsiz nusxa olishdan himoyalangan bo‘lishi lozim.

103. Elektron to‘lov hujjatlarini kirituvchi, tasdiqlovchi va elektron to‘lovlar bilan tegishli amallarni (bosh buxgalter, so‘nggi nazorat) bajaruvchi barcha mas’ul xodimlar elektron raqamli imzo bilan ta’minlangan bo‘lishlari va avtomatlashtirilgan bank tizimlarida ushbu elektron raqamli imzodan foydalanishlari zarur.

Bank tomonidan masofaviy xizmat ko‘rsatilganda, elektron to‘lov hujjatlarini kirituvchi, tasdiqlovchi va elektron to‘lovlar bilan tegishli amallarni

bajaruvchi barcha xodimlar elektron raqamli imzo bilan elektron to‘lov hujjatlarini tasdiqlashi lozim.

104. Banklar tarmoq orqali uzatilayotgan to‘lov ma’lumotlarini elektron raqamli imzo va shifrlash kalitlari qo‘llanilgan holda himoya qilinishini ta’minlaydi.

105. Elektron raqamli imzo kaliti sertifikatining amal qilish muddati elektron raqamli imzo ro‘yxatga olingan paytdan e’tiboran yigirma to‘rt oydan oshmasligi kerak. Bunda elektron raqamli imzo kaliti sertifikatining amal qilish muddati ikki martadan ko‘p bo‘lmagan muddatga uzaytirilishi mumkin.

Foydalanuvchilarning elektron raqamli imzo ochiq kalitlari avtomatlashtirilgan bank tizimida ro‘yxatga olinishi va hisobi yuritilishi kerak.

106. Elektron raqamli imzo kalitining sertifikati ro‘yxatga olish markazi orqali yaratiladi. Bunda, sertifikatga quyidagi ma’lumotlar kiritiladi:

elektron raqamli imzo yopiq kalitining egasi bo‘lgan jismoniy shaxsning familiyasi, ismi va otasining ismi;

xodimning lavozimi va shaxsini tasdiqlovchi hujjat ma’lumotlari;

jismoniy shaxsning shaxsiy identifikatsiya raqami;

elektron raqamli imzoning ochiq kaliti;

mazkur sertifikatni bergan ro‘yxatga olish markazining nomi va joylashgan manzili;

elektron raqamli imzodan foydalanish maqsadlari to‘g‘risidagi ma’lumotlar;

elektron raqamli imzolar kalitlari sertifikatlari reyestrining elektron manzili.

107. Elektron raqamli imzo va shifrlash kalitlarining yaratilish jarayonlari muhofazalanishi lozim.

108. Elektron raqamli imzoning yopiq kalitidan faqat uning egasi foydalanishi lozim.

Bank tizimidagi elektron raqamli imzo kalitlari qo‘llanilishi Xizmat tomonidan nazorat qilinadi.

Elektron raqamli imzoning yopiq kalitini ish kompyuter xotirasida yoki ish kompyuteriga doimiy ulangan holatda turuvchi tashqi xotirada saqlash taqiqlanadi.

109. Elektron raqamli imzo bilan tasdiqlanmagan va shifrlash jarayonidan o‘tmagan elektron to‘lovlar qayta ishlash uchun qabul qilinishi taqiqlanadi.

110. Markaziy bank tomonidan berilgan elektron raqamli imzo kalitlari buzilganda, yo‘qotilganda va boshqa shunga o‘xshash holatlarda banklar elektron raqamli imzoning yangilanish sabablarini ko‘rsatgan holda Markaziy bankka murojaat qiladi. Markaziy bank murojaat asosida bir kun ichida elektron raqamli imzoni yangilab beradi.

14-bob. Elektron arxivni tashkil qilish va elektron arxiv hujjatlarining tarkibi

111. Elektron arxiv bank arxivining tarkibiy bo‘linmasi sifatida tashkil qilinadi.

112. Elektron arxiv o‘zining elektron arxiv axborot tizimiga ega bo‘lishi va uning axborot resurslari shakllantirilishi lozim.

113. Elektron arxivning asosiy vazifalari quyidagilardan iborat bo‘lishi kerak:

elektron hujjatlarni jamlash, hisobga olish, ularni saqlash, shuningdek ulardan foydalanishni ta’minlash;

axborot resurslarining arxiv nusxalarini tayyorlash va ularni qonunchilik hujjatlarida belgilangan muddatlarda davlat saqloviga topshirish;

elektron hujjatlarni rasmiylashtirish bo‘yicha bankning tarkibiy bo‘linmalariga uslubiy yordam ko‘rsatish;

elektron arxiv axborot resursining axborot xavfsizligi va kiberxavfsizligini ta’minlash.

114. Elektron arxiv hujjatlari tarkibiga quyidagi axborot resurslari kirishi lozim:

bank amaliyot kunidagi elektron ma’lumotlarning to‘liq bazasi;

muddati tugagan shifrlash va elektron raqamli imzo kalitlarining ochiq kalitlari;

bank amaliyot kuni dasturlari va boshqa alohida foydalanilayotgan dasturlar majmuasi;

bank axborot tizimlari va resurslari bilan bog‘liq barcha dasturlarning, dasturiy va apparat-dasturiy qurilmalarning elektron bayonnomalari hamda noxush hodisalar bilan bog‘liq elektron bayonnomalar;

elektron pochta orqali qabul qilingan va uzatilgan to‘lovlarga tegishli (farmoyish, qaror va boshqa) hujjatlar;

shifrlangan va shifrlanmagan ko‘rinishdagi barcha kiruvchi va chiquvchi elektron to‘lov hujjatlari;

tijorat banklarining kredit va boshqa bank operatsiyalariga taalluqli ma’lumotlari;

banklarning boshqaruv, shaxsiy tarkib hujjatlari va boshqa ma’lumotlar.

115. Bankda elektron arxivda saqlanuvchi ma’lumotlar ro‘yxati shakllantirilishi va bir yilda bir marta yangilab turilishi lozim.

Banklar o‘zining siyosati, mavjud bo‘lgan axborot tizimlari va bank oldiga qo‘yilgan talablardan kelib chiqib, elektron arxivda saqlanuvchi ma’lumotlar ro‘yxatini belgilashi mumkin.

116. Elektron arxiv belgilangan vazifalarni bajarish uchun tegishli texnik qurilma-vositalar va dasturlar bilan ta’minlangan bo‘lishi kerak.

Elektron arxivning axborot resursi tashqi saqlovchilarga ko‘chirilib, seyfda yoki temir shkafda saqlanishi lozim.

117. Asosiy ish jarayonidagi ma’lumotlar va ularning xotirasida (server disklarida) saqlanayotgan ma’lumotlar elektron arxivning axborot resursi hisoblanmaydi.

118. Banklar elektron arxivning axborot resursi nusxalarini saqlash uchun kamida ikkita bir-biriga bog‘liq bo‘lmagan saqlash joylarini tashkil etishlari lozim.

Elektron arxiv har kuni dasturiy ravishda axborot resursini shakllantirishi (arxivlashi) hamda elektron axborot tashuvchi vositalarga yozilishi jarayonini elektron jurnalda qayd etib borishi lozim. Elektron jurnalda axborot resursiga ko‘chirilgan axborotlar to‘g‘risidagi (vaqti, nomi, hajmi va boshqa) ma’lumotlar hamda elektron arxiv butligini aniqlash maqsadida ushbu axborotlarning xesh summasi (nazorat raqamlari) qayd etib borilishi kerak. Elektron arxivning mas’ul xodimi ushbu ishlarni amalga oshirganligi to‘g‘risida maxsus daftarda qayd qilib boradi.

119. Bankning ichki audit xizmati xodimi har oyda kamida bir marta elektron arxivning ishlarini tekshirishi va tekshiruv natijalarini arxiv ishlarini qayd etish maxsus daftariga kiritib borishi zarur. Kamchiliklar aniqlangan taqdirda bankning ichki audit xizmati tomonidan dalolatnoma rasmiylashtirilishi va kamchiliklarni bartaraf etish choralari ko‘rilishi tashkillashtiriladi.

120. Elektron arxiv tomonidan elektron arxivning axborot resursi ma’lumotlari har olti oyda bir marta butligi yuzasidan tekshirib turiladi hamda ushbu tekshirish natijalari maxsus daftarda yuritiladi. Agar elektron arxiv axborot resurslari ma’lumotlari qisman yoki umuman buzilganligi aniqlansa, tegishli ma’lumotlar qayta tiklanishi va bu haqida dalolatnoma tuzilishi lozim.

121. Elektron arxivga topshirilgan elektron hujjatlarning (elektron resurslarning) saqlanish muddati qog‘oz asosdagi hujjatlar uchun o‘rnatilgan muddatlardan kam bo‘lmasligi lozim.

Bank tomonidan saqlanish muddati doimiy bo‘lgan elektron ma’lumotlar idoraviy arxivda o‘n besh yil mobaynida saqlangandan so‘ng ularning bir nusxasi o‘rnatilgan tartibda davlat arxivlariga topshirilishi lozim.

122. Bankning filiallari faoliyati tugatilganda, elektron arxivning axborot resursi bankning hududiy filiallariga, hududiy filiallari mavjud bo‘lmagan banklar bosh bankka belgilangan tartibda topshiriladi. Bank faoliyati tugatilib boshqa bankka qo‘shib yuborilganda, elektron arxiv ma’lumotlari qo‘shib yuborilayotgan bankning elektron arxiviga belgilangan tartibda topshiriladi.

123. Bank faoliyati tugatilganda elektron arxivning axborot resurslari davlat arxiviga topshiriladi.

124. Elektron arxiv xodim(lar)i axborot resurslarining to‘liqligi, to‘g‘ri shakllanganligi hamda ishonchliligi uchun shaxsan javobgar hisoblanadi.

15-bob. Axborot aktivlari ish jarayonlarining uzluksizligi va qayta tiklanishini ta’minlash

125. Banklar axborot aktivlari ish jarayonining uzluksizligini ta’minlashi hamda buning uchun tashkiliy va texnikaviy choralarni ko‘rishlari kerak.

Banklar axborot aktivlari ish jarayonida to‘xtashlar, texnik nosozliklar, favqulodda holatlar va katta zarar yetkazuvchi holatlar yuzaga kelganda ish uzluksizligini ta’minlashi va buning uchun tegishli choralarni avvaldan ko‘rgan bo‘lishlari lozim.

126. Bankda axborot aktivlari ish jarayonlari uzluksizligini ta’minlash bo‘yicha talablar ishlab chiqilishi, shu jumladan uzilishlar (to‘xtashlar) vaqtida amalga oshiriladigan ishlar (barcha holatlar uchun) bo‘yicha reja tasdiqlanishi kerak. Rejada ishtirok etuvchi xodimlar harakati yoritilishi va bu xodimlar tegishli tayyorgarlik ko‘rib qo‘ygan bo‘lishlari kerak.

127. Banklar axborot aktivlari quyi tizimlarini qayta tiklash tartibini ishlab chiqishi, ma’lumotlarni va tegishli dasturlarni zaxiralashi, yilda kamida ikki marotaba qayta tiklash sinov ishlarini o‘tkazishi hamda amalga oshirilgan barcha ishlarni hujjatlashtirishi lozim. Qayta tiklash rejasi barcha mavjud axborot tizimlari, operatsion tizimlar va texnik qurilmalarni inobatga olgan holda tuzilishi lozim.

128. Bank axborot tizimlarini qisqa muddatlarda qayta tiklash maqsadida tegishli elektron ma’lumotlarni shakllantirishi kerak. Bunda to‘lov tizimiga bog‘liq bankdagi barcha axborot tizimlarining qayta tiklanuvchi ma’lumotlari kechagi kun yakuniga nisbatan aktual tarzda saqlanishi tashkil etilishi kerak.

129. Qayta tiklanuvchi elektron ma’lumotlar ro‘yxati, ularni ko‘chirish (hosil qilish) vaqti va boshqalar bank tomonidan belgilanadi.

Banklar qayta tiklanuvchi elektron ma’lumotlarning himoyasini ta’minlashi lozim.

130. Bankning ichki audit xizmati har oyda kamida bir marta ma’lumotlarni qayta tiklash tizimining holatini tekshirishi va tekshiruv natijalarini maxsus daftarida qayd qilib borishi kerak. Kamchiliklar aniqlangan taqdirda, bu haqida dalolatnoma rasmiylashtirilishi lozim.

131. Axborot aktivlarining texnik vositalari ishdan chiqishi holatlari yuz berganda, tizimning beto‘xtov ishlashini ta’minlash uchun banklar zaxira tiklanish rejasi, dastur va uskunalarga ega bo‘lishlari shart.

132. Axborot aktivlaridagi serverlar va kompyuterlar ekspert tasdig‘idan o‘tgan yoki litsenziyalangan dasturlarga ega bo‘lishi lozim.

133. Bankning axborot aktivlari, axborotni himoyalash vositalari, ma’lumotlar bazasi, veb-serverlari, to‘lov tizimi va boshqa serverlari bankning ma’lumotlarni qayta ishlash asosiy va zaxira markazlarida joylashtiriladi.

Mazkur markazlar axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha talablarga qat’iy rioya etishi, shuningdek konfidensial, jumladan bank sirini tashkil etuvchi ma’lumotlarning sizib chiqishini oldini olishni hisobga olib, bankning binosida, filial(lar)ida, boshqa banklarda, Markaziy bankning bulutli texnologiya asosida yaratilgan data-markazida yoki davlat data-markazlarida tashkil etilishi mumkin.

Banklar axborot aktivlarini favqulodda (yong‘in, zilzila, suv toshqini va boshqa) holatlardan himoya qilish uchun 50 kmdan kam bo‘lmagan masofada joylashgan hududlardagi shahar markazlarida zaxira ma’lumotlarni qayta ishlash markazini tashkil etishi lozim.

134. Asosiy axborot tizimlarida ishlatilayotgan dastur va ma’lumotlarning zaxira nusxalari bankning zaxira markazida saqlanadi. Zaxira markazidagi ma’lumotlarning qayta tiklanishi (sinxronizatsiya) davriyligi kuniga bir martadan kam bo‘lmasligi kerak.

16-bob. Bankda tashkil etilgan ma’lumotlarni qayta ishlash markazlari va server xonalarining xavfsizlik talablari

135. 135. Banklarda tashkil etilgan ma’lumotlarni qayta ishlash markazlari quyidagi talablarga javob berishi lozim:

ma’lumotlarni qayta ishlash markazining provayderi tegishli litsenziya va sertifikatlarga ega bo‘lishi (PCI DSS, ISO 27001);

Tier III yoki Tier IV xalqaro standartlariga mos kelishi;

xizmat ko‘rsatish darajasini SLA (Service Level Agreement) belgilovchi hujjatning mavjudligi.

136. Bank server xonasining kafolatli elektr ta’minoti tizimini joriy etishi lozim. Bunda, turli elektr podstansiyalardan elektr ta’minotining ikkita kirishlari va bitta avtomatik tarzda ishga tushuvchi dizel elektr stansiyasi mavjud bo‘lishi kerak. Elektr energiyasining barcha uchta manbai elektr ta’minotining asosiy (zaxira) fideriga avtomatik tarzda qayta ulanishi ta’minlanishi kerak.

137. Elektr ta’minoti liniyalarining, avtomatik dizel elektr stansiyasi va uning zaxirasi avtomatik kirishining parametrlari uskuna va server xonasi tizimlarining iste’mol qilinadigan umumiy quvvatidan kelib chiqib aniqlanishi va quvvat bo‘yicha zaxiraning kamida 10 foizini ta’minlashi kerak.

138. Bank uzluksiz ishlashi uchun kamida bir sutkaga yetadigan yoqilg‘i zaxirasiga ega bo‘lgan dizel elektr stansiyasi bilan ta’minlanishi lozim, bunda bankda elektr quvvati bo‘lmaganda dizel elektr stansiyasi avtomatik ravishda ishga tushishi kerak.

139. Banklar server xonasini uzluksiz elektr ta’minoti manbai (UPS) bilan jihozlashlari lozim.

Bunda elektr ta’minoti manbai (UPS) quvvati barcha ta’minlanadigan uskuna va kelajakdagi ehtiyoj uchun zaxira hisobga olingan holda joriy qilingan bo‘lishi kerak. Elektr ta’minoti manbai (UPS) orqali avtonom ishlashda ehtiyojlar, shuningdek zaxira liniyalariga va avtomatik dizel elektr stansiyasiga o‘tish hamda qayta o‘tish uchun kerak bo‘ladigan vaqt hisobga olinadi.

140. Server xonasiga kirish faqat tasdiqlangan ro‘yxatga muvofiq amalga oshiriladi.

141. Server xonasiga kirishga ruxsat berilgan xodimlar ro‘yxatida bo‘lmagan shaxslar server xonasiga kirish zarurati paydo bo‘lgan hollarda ularning kirishi asoslangan holda talabnoma bilan rasmiylashtirilishi lozim. Ushbu talabnoma axborot texnologiyalari bo‘linmasi rahbari tomonidan ko‘rib chiqilishi va imzolanishi, shuningdek Xizmat rahbari bilan kelishilishi zarur. Server xonasiga kirish server administratori kuzatuvi ostida amalga oshiriladi.

142. Xodimlar server xonasiga nazorat qilish tizimi orqali nazoratdan o‘tgan holda (biometrik yoki boshqa usullardan) kirishi kerak.

143. Server xonasiga axborot aktivlariga xizmat ko‘rsatuvchi tashkilotlar xodimlari kiritilganda, bu haqda ro‘yxatga olish jurnaliga kirish va chiqish sanasi, vaqti, amalga oshirilgan ishlar nomi, bajaruvchining familiyasi, ismi, lavozimi, tashkilot nomi yozilishi hamda ushbu xodimning imzosi qo‘yilishi kerak.

144. Server xonasi quyidagi jihozlanish talablariga javob berishi shart:

mustahkam devorlar va ishonchli to‘siqlarga ega bo‘lishi;

ishonchli (kodli) qulflar o‘rnatilgan mustahkam eshiklar bilan jihozlanishi;

derazalar xonaga kirishdan himoya qilish vositalariga ega bo‘lishi, shuningdek begona shaxslarning ko‘z yoki maxsus qurilmalar bilan kuzatishidan himoya qiluvchi deraza pardalari, qo‘riqlash va ogohlantirish qurilmalari bilan jihozlanishi;

yong‘inga qarshi himoya tizimi va vositalari bilan jihozlanishi.

145. Server xonasiga o‘rnatilgan videokuzatuv tizimi quyidagi talablarga javob berishi kerak:

serverlar bilan bevosita jismoniy kontaktlar yozib borilishi;

uzluksiz videokuzatuv amalga oshirilishi;

serverlarning (server shkaflarining) oldi va orqa tarafini kechayu-kunduz nazorat qilish imkoniyati bo‘lishi;

videokameralarning tasvirga olish imkoniyatlari texnologik qurilmalarga xizmat ko‘rsatayotgan xodimlarning yuzlarini ishonch bilan farqlashiga yetarli

bo‘lishi.

146. Videokuzatuv qurilmalari va binoga (yo‘laklarga, xonalarga) kirishni nazorat qilish tizimlari ma’lumotlari bank to‘lov tizimi lokal tarmoqlaridan ajratilgan va tashqi ta’sirlardan himoya qilingan bo‘lishi hamda elektr ta’minoti uzilgan vaqtdan boshlab 12 soat ichida energiyaga bog‘liq bo‘lmagan holda avtonom ravishda ishlash imkoniyatiga ega bo‘lishi, shuningdek videoarxiv 2 oydan kam bo‘lmasligi lozim.

147. Videoarxiv ma’lumotlarini yuritish va foydalanish bankning xavfsizlik bo‘yicha mas’ul bo‘linmasi tomonidan amalga oshiriladi.

148. Server xonasi binoning o‘t o‘chirish tizimiga bog‘liq bo‘lmagan avtomatik gazli o‘t o‘chirish qurilmasi bilan jihozlangan bo‘lishi lozim.

Gazli o‘t o‘chirish tizimi bevosita bankning server xonasidagi maxsus jihozlangan shkafda yoki buning uchun ajratilgan maxsus xonada joylashtirilishi kerak.

Gazli o‘t o‘chirish tizimini ishga tushirish yong‘indan xabar beruvchi tutun xabargohlaridan, shuningdek xona tashqarisida, devorga pol sathidan 1,5 m balandlikda o‘rnatilgan qo‘lda ishga tushiriladigan xabargohlardan amalga oshirilishi kerak.

149. Gazli o‘t o‘chirish tizimi xonaning ichkarisida va tashqarisida joylashgan avtomatik gazli o‘t o‘chirish qurilmasi ishga tushganligi to‘g‘risida xodimlarga xabar beruvchi tabloga va xonaning tashqarisida o‘rnatilgan tovushli xabar beruvchi moslamaga ega bo‘lishi kerak.

150. Gaz va tutunni chiqarib yuborish tizimi yong‘inni o‘chirish tizimi ishga tushganidan so‘ng server xonasidan gaz va tutunning chiqib ketishini ta’minlashi kerak. Ushbu tizim binoning ventilyatsiya tizimidan alohida bino tomiga havo quvuri chiqarilgan holda bajariladi. Tizim server xonasidagi havo hajmidan uch hissa oshadigan hajmdagi gaz havo aralashmasini chiqarib tashlash imkoniyatiga ega bo‘lishi kerak.

151. Sovitish va ventilyatsiya quyi tizimiga qo‘yiladigan asosiy talablar quyidagilardan iborat:

a) server xonasida quyidagi iqlim sharoitlariga rioya qilinishi kerak:

xonadagi havo harorati 18 – 24°C;

haroratning yo‘l qo‘yiladigan og‘ishlari ± 2°C;

havoning nisbiy namligi 40 – 50 foiz;

havoni sovitish tizimining haqiqiy sovitish quvvati server xonasida joylashgan barcha uskunalar va tizimlarning umumiy issiqlik chiqarishidan ortiq bo‘lishi kerak;

b) server xonasining havosini sovitish tizimi 100 foiz zaxiralashdan foydalangan holda bajariladi (kamida, har biri mustaqil ravishda xonaning havo rejimini ta’minlay oladigan ikkita mustaqil konditsioner);

v) sovitish tizimi masofadan monitoringni amalga oshirish imkoniyatini ta’minlashi kerak.

17-bob. Bankning tashqi axborot tizimlari bilan axborot almashinuvida axborot xavfsizligi va kiberxavfsizlikni ta’minlashga qo‘yilgan talablar

152. Bank boshqa yuridik shaxsning axborot tizimi (bundan buyon matnda tashqi axborot tizimi deb yuritiladi) bilan axborot almashinuvini shartnoma asosida amalga oshiradi.

153. Bank va tashqi axborot tizimi o‘rtasida axborot almashinuvi amalga oshirilishi uchun quyidagi axborot xavfsizligi va kiberxavfsizlikni ta’minlash talablari belgilab olinishi kerak:

bank tomonidan beriladigan ma’lumotlar ro‘yxati va shakli;

bankning axborot tizimiga kirish imkoniyatlarini chegaralash chora-tadbirlari;

axborot almashinuvida autentifikatsiya va identifikatsiya jarayonlari;

elektron raqamli imzo, shifrlash va boshqa axborot muhofazasi qurilmalari, dasturlari va uskunalari;

bank siri ma’lumotlarini tashqariga chiqishining oldini olish;

mazkur Nizomda ko‘rsatilgan tarmoq xavfsizligi talablari va boshqa axborot muhofazasi talablari bajarilishi;

axborot almashinuvida qatnashuvchi xodimlarni tayinlash, ularning vazifalari, majburiyatlari va javobgarliklari.

Bank tashqi axborot tizimi bilan axborot almashinuvini boshlashdan oldin Markaziy bankni xabardor qilishi va axborot almashinuvini Markaziy bankning axborot muhofazasi bo‘yicha talablariga rioya qilgan holda amalga oshirishi shart.

18-bob. Uchinchi shaxslar bilan ishlashda xavfsizlikni ta’minlash

154. Banklar uchinchi shaxslar bilan ishlashda xavfsizlikni ta’minlash maqsadida quyidagilarni bajarishlari lozim:

uchinchi shaxslarga ma’lumotlardan foydalanish huquqini berishdan oldin xavf darajasini tahlil qilgan holda baholash;

konfidensial ma’lumotlardan foydalanish huquqi berilgan uchinchi shaxslar bilan ma’lumotlarni oshkor qilmaslik to‘g‘risidagi NDA (Non-Disclosure Agreement) kelishuvlarini imzolash;

uchinchi shaxslarga faqatgina o‘z majburiyatlarini bajarishi uchun zarur bo‘ladigan ma’lumotlar va axborot aktivlariga kirishga ruxsat berish;

uchinchi shaxslarning har bir xodimi uchun alohida foydalanuvchi akkauntini yaratish va majburiy tartibda ko‘p faktorli autentifikatsiyadan o‘tkazish;

uchinchi shaxslar bilan hamkorlik qilish tugatilganidan keyin ularda mavjud barcha konfidensial ma’lumotlarni qaytarish, yo‘q qilish hamda axborot aktivlariga kirish uchun berilgan ruxsatlar va foydalanish akkauntlarini bekor qilish.

19-bob. Bankning axborot aktivlariga masofadan ulanishda xavfsizlikni ta’minlash

155. Banklar o‘z axborot aktivlariga masofadan ulanishda quyidagi xavfsizlik choralarini ko‘rishlari lozim:

bank xodimlariga axborot aktivlariga o‘zining shaxsiy qurilmalaridan foydalangan holda masofadan turib ulanishiga ruxsat bermaslik;

xodimlarni korporativ tarmoqqa masofadan turib ulashda virtual xususiy tarmoqlardan foydalanish va ko‘p faktorli autentifikatsiyadan o‘tkazish;

masofadan turib ishlashda foydalanuvchilarning barcha harakati PAM tizimi orqali amalga oshirilishini ta’minlash;

xodimlarga masofadan turib ishlashda faqatgina o‘z vazifalarini bajarishlari uchun zarur bo‘ladigan axborot resurslaridan foydalanishiga ruxsat berish.

20-bob. Zaifliklar va konfiguratsiyalarni boshqarish

156. Banklar axborot infratuzilmalarida mavjud zaifliklarni aniqlash va bartaraf etishda quyidagilarni bajarishlari lozim:

zaifliklarni aniqlash uchun axborot aktivlarini muntazam ravishda skanerlash ishlarini olib borish;

zaifliklarni tasniflash va tavsiflashda xalqaro CVE (Common Vulnerabilities and Exposures) kabi ma’lumotlar bazalaridan foydalanish;

zaifliklarning muhimlik darajasini aniqlashda xalqaro CVSS (Common Vulnerability Scoring System) kabi baholash tizimlaridan foydalanish;

zaifliklarni bartaraf etishda kerak bo‘ladigan yangilanish va tuzatishlarni (patch) o‘rnatish;

zaifliklar holatini doimiy ravishda monitoring qilish va bank rahbariyatiga hisobot berish jarayonlarini yo‘lga qo‘yish.

157. Banklar axborot aktivlari konfiguratsiyalaring xavfsizligini ta’minlashda quyidagilarni bajarishi lozim:

axborot aktivlarining barcha tarkibiy qismlari, jumladan serverlar, ishchi stansiyalar, tarmoq qurilmalari va ilovalar uchun xavfsiz konfiguratsiyalarning asosiy liniyalarini SCB (Security Configuration Baselines) yaratish;

konfiguratsiya tavsifini unifikatsiyalashda xalqaro CCE (Common Configuration Enumeration) kabi ro‘yxatlardan foydalanish;

barcha konfiguratsiya o‘zgarishlarini tegishli tekshiruv, tasdiqlash va hujjatlashtirishdan o‘tishini ta’minlash uchun o‘zgarishlarni boshqarishning rasmiylashtirilgan jarayonlarini joriy etish;

joriy qilingan konfiguratsiyalarning belgilangan standartlar va xavfsizlik siyosatlariga muvofiqligini muntazam ravishda tekshirib borish va baholash;

konfiguratsiyalarni boshqarish jarayonlarini avtomatlashtirish va ularning belgilangan standartlarga muvofiqligini ta’minlash uchun maxsus dasturiy vositalar va platformalardan foydalanish.

21-bob. Bankning axborot tizimlari va resurslarining hayot davri bosqichlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash

158. Bankning axborot tizimlari va resurslarining hayot davri modeli quyidagi bosqichlardan iborat bo‘lishi lozim:

texnik topshiriqlarni ishlab chiqish;

loyihalash;

yaratish va sinovdan o‘tkazish;

qabul qilish va ishga tushirish;

foydalanish;

texnik xizmat ko‘rsatish va takomillashtirish;

foydalanishdan chiqarish.

159. Axborot tizimi mustaqil ravishda ishlab chiqilganda, hayot davri modelining barcha bosqichlarida axborot tizimining axborot xavfsizligi va kiberxavfsizlik talablariga muvofiqligi ko‘rib chiqishi kerak.

160. Tayyor axborot tizimi xarid qilinganda, axborot tizimining hayot davri modelining quyidagi:

qabul qilish va ishga tushirish;

foydalanish;

texnik xizmat ko‘rsatish va takomillashtirish;

foydalanishdan chiqarish bosqichlarida axborot xavfsizligi va kiberxavfsizlik talablariga muvofiqligi ta’minlanishi lozim.

161. Axborot tizimlari kiberxavfsizlik xatarlarini inobatga olingan holda loyihalanishi va ishlab chiqilishi lozim.

162. Axborot tizimi hayot davrining barcha bosqichlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash masalalariga oid ishlar Xizmat bilan kelishgan holda va uning nazorati ostida amalga oshiriladi.

163. Axborot tizimini ishlab chiqish yoki modernizatsiya qilish bo‘yicha texnik topshiriqlarda va bankning texnologik jarayonlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha talablar kiritilishi lozim.

Axborot tizimi va (yoki) uning tarkibiy qismlarini yaratish hamda sinovdan o‘tkazish bosqichlarida konfidensial, jumladan bank siriga oid ma’lumotlardan foydalanish taqiqlanadi.

Bankda dasturiy ta’minotni hayot davri bosqichlarida boshqarish platformalarining faqat lokal (on-premise) talqinlaridan (Gitlab va hokazo) foydalanishga ruxsat beriladi. Bunda, platformadagi dastur kodi avtomatik ravishda tahlil qilinishi lozim (SAST/DAST).

Bankning dasturiy ta’minotini hayot davri bosqichlarida boshqarish platformalarini internet tarmog‘iga ulash taqiqlanadi.

Bankning dasturiy ta’minotni hayot davrini boshqarish platformalariga masofadan ulanishni faqat himoyalangan VPN tarmoq orqali amalga oshirishga ruxsat beriladi.

164. Axborot tizimini ishga tushirishdan oldin ularda mavjud zaifliklar tekshirilishi shart. Barcha zaifliklar bartaraf etilganidan keyin axborot tizimini ishga tushirish mumkin.

Bankda foydalanishda bo‘lgan axborot tizimi va (yoki) uning tarkibiy qismlarida joriy etilgan himoya choralarining tavsifini o‘z ichiga olgan hujjatlar bo‘lishi shart.

165. Bankda dastur ishlab chiqaruvchilar tomonidan axborot tizimini ishlab chiqish va yetkazib berish bosqichlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash talablari qayd etilishi lozim.

Banklar dastur ishlab chiqaruvchilar tomonidan ishlab chiqilgan axborot tizimlarida amalga oshirilgan himoya choralarini tahlil qilishi va zarur hollarda qo‘shimcha talablarni belgilashlari mumkin.

Banklar axborot tizimlarini ishlab chiquvchi yoki tayyor axborot tizimlarini yetkazib beruvchi tashkilotlar bilan tuzgan shartnomalarida axborot tizimining butun xizmat muddati davomida texnik qo‘llab-quvvatlash bo‘yicha shartlarni kiritishi lozim. Agarda shartnomada mazkur shartlar ko‘rsatib o‘tilmasa, bank yetkazib beruvchidan uning ishtirokisiz axborot tizimi va uning tarkibiy qismlarini qo‘llab-quvvatlash imkoniyatini beruvchi hujjatlar to‘plamini olishi shart.

166. Axborot tizimidan foydalanish davrida quyidagi tartib-taomillar belgilanishi, bajarilishi va ro‘yxatdan o‘tkazilishi lozim:

joriy etilgan himoya choralarining ishlashi (faoliyati, samaradorligi)ni nazorat qilish, shu jumladan tashkiliy himoya choralarining amalga oshirilishini tekshirish, qo‘llanilayotgan texnik himoya choralarining tarkibi va sozlash parametrlarini kuzatib borish;

uskunalar va dasturiy ta’minotda zaif tomonlar mavjud emasligini tekshirish;

sozlash parametrlari va qo‘llanilayotgan texnik himoya choralariga o‘zgartirishlar kiritilishini nazorat qilish;

dasturiy ta’minotning, shu jumladan texnik himoya choralarning zaruriy yangilanishlarini nazorat qilish.

167. Axborot tizimidan foydalanish davrida axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha amalga oshirilgan barcha funksiyalarni tiklash uchun zarur bo‘lgan tartib-qoidalar aniqlanishi, bajarilishi, qayd etilishi va nazorat qilinishi lozim.

Axborot tizimidan foydalanish davrida o‘rnatiladigan va (yoki) foydalaniladigan dasturiy ta’minotning tarkibini nazorat qilish tartiblari belgilanishi, bajarilishi va qayd etilishi shart.

Axborot tizimidan foydalanish davrida konfidensial, jumladan bank siriga oid ma’lumotlar saqlanayotgan vositalarning xavfsizligini ta’minlash uchun zarur bo‘lgan tartib-qoidalar aniqlanishi, amalga oshirilishi va nazorat qilinishi kerak.

Axborot tizimini foydalanishdan chiqarish jarayonida bank faoliyatiga zarar yetkazishi mumkin bo‘lgan ma’lumotlar texnik himoya choralari bilan qo‘llaniladigan axborotni tiklash imkoniyatini istisno qiluvchi algoritmlar va (yoki) usullar yordamida axborot tizimlarining doimiy xotirasidan hamda tashqi tashuvchilardan o‘chiriladi, bundan qonunchilikda belgilangan va shartnomaviy hujjatlarda qayd etilgan muddatlar davomida saqlanishi ko‘zda tutilgan elektron hujjat arxivlari va bayonnomalar (loglar) mustasno.

22-bob. Data-markazlar xizmatlaridan foydalanishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha talablar

168. Banklar o‘zining ma’lumotlarni qayta ishlash bo‘yicha asosiy va zaxira markazlarini quyidagi talablarga muvofiq bo‘lgan data-markazlarga joylashtirishlari mumkin:

axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha xalqaro ISO/IEC 27001, PCI DSS sertifikatlari va (yoki) axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha boshqa xalqaro sertifikatlarning mavjud bo‘lgan;

SOC 2 standartiga muvofiq bo‘lgan;

Tier III yoki Tier IV xalqaro standartlariga mos keladigan;

xizmat ko‘rsatish darajasini belgilovchi SLA hujjati mavjud bo‘lgan;

uzluksiz ishlash vaqtida (uptime) va nosozliklar ro‘y berganda, qayta tiklash muddatlari kafolatlangan;

kirish nazorati, videokuzatuv, qo‘riqlash xizmati va tabiiy ofatlardan himoyalanish kabi xavfsizlik choralari mavjud bo‘lgan;

turli aloqa kanallari (telefon, elektron pochta, chat) orqali kun-u tun (24/7) faoliyat yurituvchi texnik yordam xizmatiga ega bo‘lgan;

data-markaz administratorlari tomonidan ko‘p omilli autentifikatsiya va minimal imtiyozlar tamoyiliga asoslangan kirish boshqaruv tizimi mavjud bo‘lgan;

banklarga o‘z ma’lumotlariga kirish va so‘rov bo‘yicha ma’lumotlarni o‘chirish imkoniyati yaratilgan;

muntazam ravishda axborot xavfsizligi va kiberxavfsizlik auditlari o‘tkaziladigan hamda natijalari banklarga taqdim etiladigan;

yangi tahdidlardan himoyalanish uchun dasturiy ta’minot va texnologiyalarni o‘z vaqtida yangilab boradigan;

Markaziy bankka tekshiruvlar o‘tkazish imkoniyati yaratilgan;

kirish qaydnomalari (loglar) va o‘zgarishlarni kamida 5 yil davomida saqlash imkoniyati yaratilgan;

zaifliklarni tahlil qilish va xavfsizlik sinovlari (pentestinglar) yiliga kamida bir marotaba o‘tkaziladigan;

biznesning uzluksizligini ta’minlaydigan va qayta tiklanish rejalarining samaradorligini tekshirish uchun muntazam ravishda sinovdan o‘tkazib turish ishlari yo‘lga qo‘yilgan.

169. Data-markazlar o‘z xodimlariga muntazam ravishda axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha mashg‘ulotlar o‘tkazib turishi lozim.

170. Data-markaz administratorlari barcha o‘zgartirishlarni bank bilan kelishilgan holda PAM tizimi orqali amalga oshirishi lozim.

Data-markaz zamonaviy keyingi avlod tarmoqlararo ekranlarning apparat-dasturiy vositalari bilan muhofazalangan bo‘lishi kerak.

171. Data-markazlar banklarning ma’lumotlarini qayta ishlash markazlarining axborot xavfsizligi va kiberxavfsizligini ta’minlash tizimlarini Markaziy bank “CERT-CBU” kiberxavfsizlik markazi monitoring tizimiga ulashi shart.

172. Banklar o‘zining ma’lumotlarni qayta ishlash bo‘yicha zaxira markazlarini data-markazlarga joylashtirishda ularda axborot xavfsizligi va

kiberxavfsizlikni ta’minlash majburiyatini ko‘zda tutishi lozim.

173. Banklar o‘zining ma’lumotlarni qayta ishlash markazlarining joylashuv manzili o‘zgarganligi to‘g‘risida zudlik bilan Markaziy bankka xabar berishi lozim.

23-bob. Axborot xavfsizligi va kiberxavfsizlikni ta’minlash bo‘yicha talablar ustidan nazorat

174. Bank axborot xavfsizligi va kiberxavfsizlikning ta’minlanganlik darajasini aniqlash maqsadida tashqi tashkilotlar xizmatidan foydalanishi va ichki auditini amalga oshirishi mumkin.

175. Tashqi tashkilot xizmatlari audit yoki ekspertiza ko‘rinishida amalga oshirilishi mumkin. Bank audit yoki ekspertiza ishlarini o‘tkazuvchi tashkilotlarga konfidensial, shu jumladan bank siri ma’lumotlarini taqdim etish yuzasidan ichki hujjat ishlab chiqishi lozim. Bunda, ushbu ma’lumotlar tegishli shartnoma asosida berilishi kerak.

176. Bosh bankning Xizmati bank va uning filiallarida mazkur Nizom talablarining bajarilishi ustidan doimiy nazorat olib borishi lozim.

24-bob. Yakuniy qoida

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

O‘zbekiston
Respublikasi
Markaziy banki boshqaruvining
2025-yil 1-avgustdagi
19/1-son qaroriga
2-ILOVA

O‘z kuchini yo‘qotgan deb topilayotgan idoraviy normativ-huquqiy hujjatlar RO‘YXATI

1. O‘zbekiston Respublikasi Markaziy banki boshqaruvining 2020-yil 25-yanvardagi 2/4-son “O‘zbekiston Respublikasi tijorat banklari avtomatlashtirilgan bank tizimlarida axborotni muhofaza qilish to‘g‘risidagi nizomni tasdiqlash haqida”gi qarori (ro‘yxat raqami 3224, 2020-yil 10-mart) (Qonun hujjatlari ma’lumotlari milliy bazasi, 10.03.2020-y., 10/20/3224/0312-son).

2. O‘zbekiston Respublikasi Markaziy banki boshqaruvining 2021-yil 28-maydagi 12/3-son “O‘zbekiston Respublikasi tijorat banklari avtomatlashtirilgan bank tizimlarida axborotni muhofaza qilish to‘g‘risidagi nizomning 1-bandiga o‘zgartirish kiritish haqida”gi qarori (ro‘yxat raqami 3224-1, 2021-yil 17-iyun) (Qonunchilik ma’lumotlari milliy bazasi, 17.06.2021-y., 10/21/3224-1/0567-son).

3. O‘zbekiston Respublikasi Markaziy banki boshqaruvining 2023-yil 21-yanvardagi 1/13-son “O‘zbekiston Respublikasi tijorat banklari avtomatlashtirilgan bank tizimlarida axborotni muhofaza qilish to‘g‘risidagi nizomga o‘zgartirishlar kiritish haqida”gi qarori (ro‘yxat raqami 3224-2, 2023-yil 31-yanvar) (Qonunchilik ma’lumotlari milliy bazasi, 01.02.2023-y., 10/23/3224-2/0064-son).