“O’ZBEKISTON SANOAT-QURILISH BANKI” AKSIYADORLIK TIJORAT BANKIАКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК “УЗБЕКСКИЙ ПРОМЫШЛЕННО-СТРОИТЕЛЬНЫЙ БАНК”

BOSHQARUV QARORI

Toshkent sh. **№ 97** **02.05.2023**

“O’zbekiston sanoat - qurilish banki” Aksiyadorlik tijorat bankining

axborot xavfsizligi siyosati”ni yangi tahrirda ma’qullash haqida

O‘zbekiston Respublikasi Adliya vazirligida 2020-yil 10-martda 3224-son bilan ro‘yxatga olingan “O’zbekiston Respublikasi tijorat banklari avtomatlashtirilgan bank tizimlarida axborotni muhofaza qilish to’g’risidagi” Nizomning 11 - bandida Bank axborot xavfsizligiga oid ichki siyosatini ishlab chiqishi va qabul qilishi lozimligi belgilangan.

Amaldagi “O’zsanoatqurilishbank” ATBning axborot xavfsizligi siyosati Bank boshqaruvining 2017-yil 13-iyuldagi 149 - sonli qarori bilan ma’qullangan.

O’zbekiston Respublikasi Davlat xavfsizlik xizmati va “Kiberxavfsizlik markazi” DUK tomonidan “O’zsanoatqurilishbank” ATBning axborot tuzilmasida axborot va kiberxavfsizlikni ta’minlanganlik holati yuzasidan olib borilgan tekshiruv natijasida aniqlangan kamchiliklarni bartaraf etish bo’yicha tasdiqlangan chora-tadbirlar rejasining 1-bandi ijrosi yuzasidan, hamkorlikda “O’zbekiston sanoat – qurilish banki” Aksiyadorlik tijorat bankining axborot xavfsizligi siyosati” yangi tahrirda ishlab chiqildi va Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining 2022-yil 10-noyabrdagi 27-8/7558-sonli hamda Davlat xavfsizlik xizmatining 2023-yil 24-fevraldagi 14/2148-sonli xatlari bilan uning loyihasi kelishildi.

Shu munosabat bilan, Xavfsizlik va axborotlarni muhofaza qilish departamenti va tegishli tarkibiy bo‘linmalar bilan kelishilgan “O’zbekiston sanoat - qurilish banki” Aksiyadorlik tijorat bankining axborot xavfsizligi siyosati” yangi tahriri o‘rnatilgan tartibda Boshqaruv muhokamasiga kiritilgan.

Bank kuzatuv kengashi to‘g‘risidagi Nizomga asosan, Bankning ichki siyosatlari va ularga kiritiladigan o‘zgartirish hamda qo‘shimchalarni tasdiqlash Bank kuzatuv kengashi vakolatiga kiradi.

Bank boshqaruvi to‘g‘risidagi Nizomning 23-bandida Bank kuzatuv kengashi va Aksiyadorlarning umumiy yig‘ilishi vakolatiga kiritilgan barcha masalalar, odatda dastlabki tarzda Boshqaruv tomonidan ko‘rib chiqilishi belgilangan.

Yuqoridagilardan kelib chiqib, Bank boshqaruvi

QAROR QILADI:

1. “O’zbekiston sanoat - qurilish banki” Aksiyadorlik tijorat bankining axborot xavfsizligi siyosati” (yangi tahrirda) mazkur qarorning ilovasiga muvofiq ma’qullansin va tasdiqlash uchun Bank kuzatuv kengashi muhokamasiga kiritilsin.

Shu munosabat bilan, Bank boshqaruvining 2017-yil 13-iyuldagi 149-sonli qarori bilan ma’qullangan “O’zsanoatqurilishbank” ATBning axborot xavfsizligi siyosati” o’z kuchini yo’qotgan deb hisoblansin.

2. Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori (S.Sergienko) mazkur Siyosat Bank kuzatuv kengashi tomonidan tasdiqlangandan so’ng, Bankning barcha tarkibiy bo’linmalarga yetkazilishi hamda ular bo’yicha texnik o’quv o’tkazilishini ta’minlasin.

3. Barcha tarkibiy bo’linma rahbarlari kelishilgan “O’zbekiston sanoat - qurilish banki” Aksiyadorlik tijorat bankining axborot xavfsizligi siyosati” mazmun-mohiyatini xodimlarga yetkazsin va uning talablari xodimlar tomonidan to’liq bajarilishini ta’minlasin.

4. Yuridik departament Metodologiya boshqarmasi (S.Raxmatullayev) mazkur qaror bilan ma’qullanayotgan ichki me’yoriy hujjat Bank kuzatuv kengashi tomonidan tasdiqlangandan so‘ng, uni qonunchilikda belgilangan muddatda Markaziy bankka yetkazsin.

5. Ushbu qaror ijrosini nazorat qilishni o’z zimmamda qoldiraman.

Boshqaruv Raisi
Annaklichev Saxi Saparmuxamedovich

Akbarjonov A.A. Yakubov Sh.I. A.A.Ergashev
B.N.Norxujayev S.N.Gulturayev X.G.Akbarov
O.R.Voxidov S.V.Sergiyenko

“O‘ZBEKISTON SANOAT-QURILISH BANKI”
AKSIYADORLIK TIJORAT BANKI
“O‘ZSANOATQURILISHBANK” ATB

“O’ZBEKISTON SANOAT – QURILISH BANKI” AKSIYADORLIK TIJORAT BANKINING AXBOROT XAVFSIZLIGI SIYOSATI

TOSHKENT – 2023 yil

MUNDARIJA

"O‘zsanoatqurilishbank" ATB
Boshqaruvining
2023-yil "2" may dagi
_____ -sonli qarori
- ilovasiga muvofiq
"MA'QULLANGAN"

Yuridik departament
Metodologiya boshqarmasida
2023-yil "10" iyul da
554 -son bilan
"RO‘YXATGA OLINGAN"

"O‘zsanoatqurilishbank" ATB
Kuzatuv kengashining
2023-yil "20" iyun dagi
_____ -sonli qarori bilan
TASDIQLANGAN

"O'zbekiston sanoat – qurilish banki" Aksiyadorlik tijorat bankining axborot xavfsizligi siyosati

(Yangi tahrirda)

I. Umumiy qoidalar

1. "O'zbekiston sanoat - qurilish banki" Aksiyadorlik tijorat banki (keyingi o‘rinlarda - bank)ning axborot xavfsizligi siyosati (keyingi o‘rinlarda - siyosat) O‘zbekiston Respublikasining "Banklar va bank faoliyati to‘g‘risida"gi, "Bank siri to‘g‘risida"gi, "Axborotlashtirish to‘g‘risida"gi "Elektron hujjat aylanishi to‘g‘risida"gi "Avtomatlashtirilgan bank tizimida axborotni muhofaza qilish to‘g‘risida"gi, "Tijorat siri to‘g‘risida"gi, "Elektron hukumat to‘g‘risida"gi "Shaxsga doir ma'lumotlar to‘g‘risida"gi Qonunlari, O‘zbekiston Respublikasi Prezidentining 2018 yil 21 noyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida"gi PQ-4024-sonli va 2019 yil 14 sentyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida"gi PQ-4452-son qarorlari, "Markaziy bank tomonidan tijorat banklarining ichki me'yoriy hujjatlariga qo‘yiladigan talablar to‘g‘risida"gi (ro‘yxat raqami: 916, 2000 yil 5 aprel), "Tijorat Banklarida korporativ boshqaruv to‘g‘risida"gi nizomlar (ro‘yxat raqami: 3254, 2020 yil 30 iyun) hamda boshqa normativ-huquqiy hujjatlarga muvofiq ishlab chiqilgan.

2. Siyosatda quyidagi atamalar va ta'riflar ishlatilgan:

avtomatlashtirilgan bank tizimi (ABT) - ma'lum funksiyalarni bajarish uchun axborot, Banki texnologiyalarini joriy qiluvchi, Bankdagi jarayonlarni avtomatlashtirish vositalari va xodimlaridan iborat tizim;

axborot resurslari - axborot tizimi tarkibidagi elektron shakldagi axborotlar, ma'lumotlar banklari, ma'lumotlar bazasi;

axborot tizimi - axborotlarni yig'ish, saqlash, izlash, ishlash va ulardan foydalanish imkonini beruvchi axborot resurslari, axborot texnologiyalari va aloqa vositalarining tashkiliy tartibga solingan yig'indisi;

axborot xavfsizligi insidenti - axborot xavfsizligining yagona voqeasi yoki bir qator noxush yoki kutilmagan voqealari bo'lib, ushbu voqealar tufayli biznes taalluqli axborotni kompromentatsiya qilish, axborot xavfsizligiga tahdidlar ehtimoli;

axborotlashtirish obyekti - turli daraja va maqsadlardagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotni qayta ishlash texnik vositalari, bu vositalar o'rnatilgan va ekspluatatsiya qilinadigan xonalar, shuningdek, muzokaralar, shu jumladan, konfidensial muzokaralar olib borish uchun mo'ljallangan xonalar;

axborot xavfsizligini boshqarish tizimi (AXBT): axborot xavfsizligini ishlab chiqish, joriy qilish, uning ishlashi, monitoringi, tahlili, unga xizmat ko'rsatish va uni takomillashtirish uchun mo'ljallangan biznes risklarni baholash usullaridan foydalanishga asoslangan umumiy boshqarish tizimining qismi;

axborotni muhofaza qilish vositalari (AMV) – texnik, kriptografik va shunga o'xshash boshqa axborotni muhofaza qilishning samaradorligini oshirish va nazorat qilish vositalari;

bank siri - bank tomonidan himoyalangan quyidagi ma'lumotlar:

o'z mijozlarining (korrespondent) operatsiyalari, hisobvaraqlari va depozitlari to'g'risida;

mijozlar (korrespondent) va ularga bank xizmatlarini ko'rsatish munosabati bilan bank tomonidan olingan ma'lumotlar;

mijozning (korrespondent) seyflarida va bank binolarida saqlanayotgan mol-mulklari mavjudligi, xususiyati va qiymati to'g'risidagi;

banklararo bitimlar va mijoz (korrespondent) nomidan yoki uning foydasiga tuzilgan bitimlar;

banklar o'rtasida bank sirini tashkil etuvchi ma'lumotlarning aylanishi natijasida ma'lum bo'lgan boshqa bankning mijozi (korrespondenti) to'g'risidagi ma'lumotlar;

buzg'unchi - axborot tizimi va uning resurslaridan ruxsat etilmagan tarzda foydalana olishdan manfaatdor bo'lgan va ruxsatsiz olish yoki o'zgartirish uchun oldindan o'ylab, ataylab harakat qilgan shaxs yoki tashkilot;

dasturiy ta'minot - ma'lumotlarni qayta ishlash tizimi va dasturiy hujjatlarni ishlatish zarur bo'lgan dasturlar to'plami;

konfidensial axborot - Davlat sirlaridan iborat ma'lumotlarga ega bo'lmagan hujjatlashtirilgan axborot, undan foydalanish qonun hujjatlariga muvofiq chegaralanadi;

ma'lumotlar bazasi - obyektiv shaklda ifodalangan va bu ma'lumotlar elektron hisoblash mashinalari yordamida to'planadigan va qayta ishlash tarzda tizimlashtirilgan ma'lumotlar (moddalar, hisob-kitoblar) jamlamasi;

nazorat qilinadigan zona - doimiy yoki bir martalik ruxsati bo‘lmagan begona shaxslar va transport vositalarining nazoratsiz bo‘lishi taqiqlangan joy (hudud, bino, binoning bir qismi);

Eslatma: Nazorat qilinadigan zonaning chegarasi quyidagilar bo‘lishi mumkin:

tashkilotning nazorat qilinadigan hududining perimetri;

muhofaza qilinadigan binoning yoki binoning qo‘riqlanadigan qismining o‘rab turgan inshootlari, agar u himoyalanmagan hududda joylashgan bo‘lsa.

risklarni baholash - risk mohiyatini aniqlash maqsadida bajariladigan, hisoblangan risk va risk mezonlarini taqqoslash jarayoni;

risk - muayyan tahdidni amalga oshirishda ma’lumotlarni qayta ishlash tizimining muayyan zaifligidan foydalanish imkoniyati;

risk tahlili - ma’lumotlarni qayta ishlash tizimi resurslarini, ushbu resurslarga tahdidlarni va ushbu tahdidlarga tizim zaifligini identifikatsiya qilish jarayonlarining muntazam bajarilishi;

ruxsatsiz foydalana olish - tizimda belgilangan foydalana olishni cheklash qoidalarini buzgan holda subyektning obyektdan yoki axborotdan foydalana olishi;

shaxsga doir ma’lumotlar - shaxsini aniqlashga imkon beradigan faktlar, voqealar va holatlar to'g'risidagi ma'lumotlar;

tahdid - kompyuter xavfsizligining potensial buzilishi;

tijorat siri - ilmiy-texnikaviy, texnologik, ishlab chiqarish, moliyaviy, iqtisodiy va boshqa sohalarda tijorat ahamiyatiga ega bo'lgan, uchinchi shaxslarga qonuniy asosda erkin foydalanish imkoni bo’lmagan ma'lumotlar;

zaiflik - ma’lumotlarni qayta ishlash tizimidagi kamchilik, undan foydalanish uning yaxlitligini buzishi va noto‘g‘ri ishlashiga olib kelishi mumkin bo’lgan holat**.**

3. Siyosatda quyidagi belgilar va qisqartmalardan foydalanilgan:

IDPS - (Intrusion Detection & Prevention System) – hujumlarni aniqlash va bartaraf etish vositasi (tizimi);

DLP - (Data Leak Prevention) - axborot tizimidan axborot chiqib ketishining oldini olish tizimi;

PAM - (Privileged Account Management) – imtiyozli foydalanuvchilarni boshqaruv tizimi;

SAN - (Storage Area Network) – ma'lumotlarni saqlash tarmog’i;

SIEM - (Security information and event management) – axborot xavfsizligi hodisalarini monitoring qilish va boshqarish tizimi;

SWIFT - (Society for Worldwide Interbank Financial Telecommunications)- Butunjahon Banklararo moliyaviy telekommunikatsiyalar jamiyati;

VPN - (Virtual Private Network) - Shaxsiy himoyalangan tarmoq;

ABT - Bankning avtomatlashtirilgan axborot bank tizimi;

BTT - O‘zbekiston Respublikasi Markaziy bankining telekommunikatsiya tarmog‘i;

AKT - axborot-kommunikatsiya texnologiyalari;

AB - Bank amaliyot boshqarmasi;

AKH - axborotni kriptografik himoyalash vositalari;

KNBT - kirish nazoratini boshqarish tizimi;

AXBT - axborot xavfsizligini boshqarish tizimi;

MBBT – ma’lumotlar bazasini boshqarish tizimi;
MBXO - mintaqaviy bank xizmatlari ofisi;
BXM - bank xizmatlari markazi;
MQIM – ma’lumotlarni qayta ishlash markazi;
ERI – elektron raqamli imzo.

II. Foydalanish sohasi

4. Siyosat himoya qilishning maqsad va vazifalarini, faoliyat davomida axborot xavfsizligi sohasidagi qoidalar, tartiblar, amaliyot va ko‘rsatmalarni belgilaydi. Siyosat bankda axborot xavfsizligini ta’minlashning asosiy huquqiy, tashkiliy, texnologik, protsessual va boshqa jihatlarini ko‘rib chiqilgan.

5. Siyosatdan bank tomonidan integratsiyalashgan AXBTni yaratish, shu jumladan bankda axborot xavfsizligi ichki me’yoriy hujjatlarni ishlab chiqish, tashkiliy-texnik va boshqa chora-tadbirlarni ko‘rish uchun asos sifatida foydalanilishi lozim.

6. Siyosat talablari axborotni qayta ishlash, saqlash va uzatish uchun barcha ma’lumotlar va manbalarga nisbatan qo‘llaniladi, davlat sirlarini o‘z ichiga olgan ma’lumotlar bundan mustasno. Davlat sirlarini o‘z ichiga olgan ma’lumotlarning himoyasi qonun hujjatlariga muvofiq ta’minlanadi.

7. Mazkur siyosatga rioya qilish bankning barcha tarkibiy bo‘linmalari va tarmoqlari xodimlari tomonidan bajarilishi majburiydir.

bank hamda unga kiritilgan tarmoqlari, MBXO va BXMning tashkiliy tuzilmasi 20-ilovada keltirilgan.

8. Siyosat talablari quyidagilarga qo'llaniladi:

bankning barcha axborot tizimlari va resurslari;

bankning barcha xodimlari (doimiy, vaqtinchalik, shartnoma asosida va boshqalar), ish joyi va lavozimidan qat’i nazar;

bank bilan o‘zaro aloqada bo‘lgan uchinchi shaxslar (bank mijozlari, yetkazib beruvchilar, pudratchilar, auditorlar, baholovchilar, tashrif buyuruvchilar, xizmat ko‘rsatuvchi xodimlar, axborot tizimlaridan tashqi foydalanuvchilar va boshqalar) u yoki bu sabablarga ko‘ra binolar va inshootlardagi xonalardan qonuniy foydalanish huquqiga ega bo‘lgan shaxslar; shu jumladan, bank axborot resurslari va tizimlaridan foydalanuvchilar.

9. Bank tarkibiy bo‘linmalari va tarmoqlarning rahbarlari mazkur siyosat qoidalariga rioya etilishi ustidan muntazam monitoring olib borilishini ta’minlaydi. Bundan tashqari, bankning Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan bank xodimlari mazkur siyosat talablariga rioya etilishi ustidan nazorati qilishlari hamda rahbariyatga mazkur tekshirish natijalari to‘g‘risida hisobot taqdim etgan holda davriy tekshiruv o‘tkaziladi.

III. Maqsad va vazifalar

10. Bankning axborot xavfsizligini ta’minlash maqsadlari quyidagilar:

bank xizmatlaridan foydalanuvchilarini (keyingi o‘rinlarda - bank mijozlari

deb yuritiladi) hamda xizmat ko'rsatuvchilar, axborot xavfsizligiga tasodifiy yoki qasddan tahdid qilish orqali yetkazilishi mumkin bo'lgan moddiy, jismoniy, ma'naviy yoki boshqa zararlardan himoya qilish, bank faoliyatiga oid axborotlarning konfidensialligi, yaxlitligi va ochiqligini ta'minlash, muhim axborot resurslari, axborot tizimlari va boshqa axborotlashtirish vositalarining ishlashini ta'minlash;

axborot xavfsizligi sohasidagi qonun hujjatlari, yo'riqnomalar va nizomlarga hamda siyosatga rioya qilinishini ta'minlash;

tijorat yoki bank sirlarini, shaxsiy ma'lumotlarni yoki boshqa konfidensial ma'lumotlarni oshkor etmaslik bo'yicha subyektlari va bank mijozlarining axborot munosabatlariga qonuniy huquqlarini himoya qilish;

bank xizmatlarini ko'rsatish bo'yicha o'z faoliyatini muvaffaqiyatli va uzluksiz amalga oshirishni ta'minlash maqsadida bank axborotlashtirish obyektlarini barqaror va ishonchli ishlashi uchun axborot xavfsizligi tahdidlaridan himoya qilish;

bankning biznes jarayonlarida foydalaniladigan bank axborot aktivlarini himoya qilish.

11. Bankning axborot xavfsizligi maqsadlariga erishish uchun axborot xavfsizligini ta'minlash vazifalari:

bankda tadbirkorlik, qonunchilik va me'yoriy hujjatlar talablariga muvofiq AXBTni yaratish va rivojlantirish;

bankning axborotlashtirish obyektlari va himoyalangan axborotni turli tahdidlardan himoya qilish, shuningdek, axborot xavfsizligi risklarini kamaytirish uchun axborot xavfsizligini boshqarishning samarali usullari va vositalarini joriy etish;

axborot xavfsizligiga tahdidlarni o'z vaqtida aniqlash va bartaraf etish maqsadida xavfsizlik holati doimiy monitoringini ta'minlash;

axborot xavfsizligi tahdidlariga tezkor javob berish mexanizmi va sharoit yaratish;

foydalanuvchilar va bank xodimlarining xabardorlik darajasini, shuningdek, bankda axborot xavfsizligi sohasidagi mutaxassislarning malaka darajasini oshirish, ularning axborot xavfsizligini boshqarish jarayonlariga jalb etishni ta'minlash;

bank axborotini qayta ishlash jarayonida foydalanuvchilar va xodimlar tomonidan ularni himoya qilish talablariga rioya etilishi ustidan nazoratni ta'minlash;

bank axborotlashtirishning muhim obyektlari xavfsizligi va ishonchli ishlashi darajasini oshirish.

IV. Asosiy qoidalar

12. Siyosat axborotni himoya qilishning tashkiliy, texnikaviy va boshqa usullari va vositalaridan foydalangan holda axborot xavfsizligini ta'minlaydi, shuningdek, axborot xavfsizligi sohasida amalga oshirilayotgan chora-tadbirlar samaradorligini har tomonlama doimiy monitoringini amalga oshiradi.

13. Axborot xavfsizligi ta'minlanishida siyosat quyidagi asosiy tamoyillarga asoslanadi:

qonuniylik - O'zbekiston Respublikasi Konstitutsiyasi va qonunchiligiga, foydalanuvchilarning qonuniy huquqlariga, amaldagi qonunlar va normativ hujjatlar talablariga qat'iy muvofiq ravishda axborot xavfsizligi choralarini amalga oshirish;

jalb qilish – bank rahbariyati va barcha xodimlari axborot xavfsizligini ta'minlash jarayonida ishtirok etadilar;

vazifalarni taqsimlash - axborot xavfsizligini ta'minlash masalalaridagi rol va javobgarliklarni bank xodimlari o'rtasida aniq taqsimlash lozim;

shaxsiy javobgarlik – mehnat shartnomalari va xodimlarning lavozim yo'riqnomalarida, shuningdek bank xodimlar bilan tuzilgan boshqa turdagi shartnomalarda (bitimlarda) kiritilgan axborot xavfsizligi talablariga rioya etilishi uchun shaxsan javobgardirlar;

professionallik - axborot xavfsizligini ta'minlash uchun mas'ul bo'lgan bank xodimlarining bilim darajasi, kasbiy darajasi doimiy ravishda takomillashtirilishi va axborot xavfsizligini boshqarish jarayonlarida qo'llanilishi kerak;

o'zaro hamkorlik va harakatlarning muvofiqligi - axborot xavfsizligini ta'minlash bo'yicha harakatlar manfaatdor idoralar bilan kelishilgan holda amalga oshirish, shuningdek, maqsadlar, vazifalar, prinsiplar va vositalar bo'yicha o'zaro hamkorlikda ish olib borishi;

iqtisodiy maqsadga muvofiqligi – bankda axborot xavfsizligini ta'minlash chora-tadbirlarini amalga oshirish xarajatlarini, axborot xavfsizligiga tahdidlarning yuzaga kelish ehtimolini va tahdid yuzaga kelganda yuzaga kelishi mumkin bo'lgan yo'qotishlar miqdorini hisobga olgan holda tanlash;

kuchaytirilgan himoya - axborot xavfsizligini ta'minlash bo'yicha chora-tadbirlar tahdidlarning barcha turlaridan samarali himoya qilishni tashkil etish zarurligini hisobga olgan holda tanlanishi kerak;

tizimli yondashuv - bank AXBTni qurishda, axborot xavfsizligini ta'minlash masalasini tushunish va hal qilish uchun muhim bo'lgan barcha ta'sir qiluvchi va vaqtni o'zgartiruvchi elementlar, shartlar va omillar hisobga olinishi kerak;

to'liqlilik - himoyaning bir xil bo'lmagan usullari va vositalaridan foydalanish kerak, ular birgalikda zaif nuqtalarni o'z ichiga oladi va barcha muhofaza qilinadigan bank obyektlarning himoyasini ta'minlaydi;

himoyaning uzluksizligi - axborot xavfsizligini ta'minlash jarayoni o'z vaqtida doimiy bo'lishi va bankning barcha darajalarida bo'lishi kerak;

ko'p bosqichli himoya – axborot xavfsizligini boshqarish jarayonlari bankning barcha darajalari va bo'g'inlarida amalga oshirilishi kerak;

hisobot berish va xatti-harakatlarning hisobi - bank xodimlari tomonidan axborot xavfsizligi bo'yicha qabul qilingan talablarning bajarilishini monitoring qilish, xodimlarning axborot aktivlariga kirishini ta'minlash va boshqarish, xodimlarning axborot aktivlari bilan bog'liq barcha harakatlarini hisobga olish.

V. Himoya obyektlari

14. Bankning axborot xavfsizligining asosiy obyektlari quyidagilar hisoblanadi:

1) Bankning konfidensial ma'lumotlari:

bankda xizmat (ishga taalluqli) ma'lumotlar;

bankning tijorat sirini tashkil etuvchi ma'lumotlar, kelishuv va shartnomalari mavjud bo'lgan mijozlar hamda kontragentlar to'g'risidagi ma'lumotlar;

bank tizimidagi bank sirini tashkil etuvchi ma'lumotlar;

bank xodimlari va mijozlarining shaxsga doir ma’lumotlari;

to‘lov ma’lumotlari va to‘lov tizimlarining hujjatlari.

2) Bank texnologik jarayonlari, shuningdek axborot va to'lov jarayonlarini:

3) Xodimlar;

bank mijozlari;

bank xodimlari;

bank axborot tizimlari dasturiy ta'minot ishlab chiqaruvchilari.

4) Ishchi stansiyalari, serverlar, ma’lumotlar bazalari va ma’lumotlarni qayta ishlash va saqlovchi boshqa vositalar.

5) Bankomatlar, kiosklar, to‘lov terminallari va elektron to‘lov moslamalari.

6) Dasturiy ta'minot: operatsion tizimlar, amaliy dasturlar va ilovalar, manba kodlari, ma'lumotlar bazasini boshqarish tizimlari (keyingi o'rinlarda AXBT), diagnostika dasturlari, ishlab chiqish vositalari va yordamchi dasturlar.

7) Xizmatlar va axborot almashish tizimlari:

a) bank bosh ofisi, MBXO, BXM va Markaziy banki xodimlari uchun bankning asosiy ma’lumotlarni qayta ishlash markazi (keyingi o‘rinlarda - MQIM) bankka tegishli server xonada joylashgan pochta serveridan foydalangan holda korporativ elektron pochta;

b) bank doirasida xodimlar o‘rtasida shuningdek, O‘zbekiston Respublikasi Markaziy banki bilan ma’lumotlar almashish uchun mo‘ljallangan banklararo elektron pochta tizimi;

c) bankda elektron ish yuritish va ijro faoliyatini nazorat qilish uchun elektron hujjat aylanishi tizimi (keyingi o‘rinlarda - EHAT tizimi deb yuritiladi). Bank xodimlari EHAT tizimining foydalanuvchilari hisoblanadi.

d) bank ichida korporativ telefon aloqalarini tashkil etish uchun bank asosiy ma’lumotlarni qayta ishlash markazi server xonasida joylashgan apparat-dasturiy ip telefoniya, shuningdek, bank mijozlari bilan o‘zaro hamkorlikda bo’lish uchun IP telefoniya tizimi “Aloqa markazi” (operator ish o‘rinlari);

e) bankning alohida apparat-dasturiy kompleksdan foydalangan holda videokonferensaloqa tizimi;

f) Bankning ijroni nazorat qilish departamenti va tarkibiy bo‘linmalari xodimlari uchun tashkil etilgan E-xat xavfsiz elektron pochtasi.

Yuqoridagi axborot almashish tizimlarining serverlari va apparat-dasturiy komplekslari bankning asosiy va zaxira ma’lumotlarni qayta ishlash markazlarining (keyingi o‘rinlarda MQIM deb yuritiladi) server xonasida joylashgan.

8) Bank tarmoq infratuzilmasi:

a) bank korporativ tarmog‘i quyidagilardan iborat:

bankda bitta domen ostida yagona boshqariladigan tarmoqni tashkil qilingan server domeni kontrolleri;

korporativ tarmoq kommutator yadrosi, marshrutizatorlar, asosiy ma'lumotlarni qayta ishlash markazini, bosh ofis, MBXO, BXM, masofaviy kassalarni korporativ tarmoqqa ulash uchun modemlar;

korporativ tarmoqni tashkil etish kanallari, korporativ tarmoqni tashqi tarmoqlarga ulash kanallari (O‘zbekiston Respublikasi Markaziy bankining

telekommunikatsiya tarmog‘i (keyingi o‘rinlarda – BTT);

ma'lumotlar bazasi serverlari hamda asosiy va zaxira ma'lumotlarni qayta ishlash markazlarining saqlash tizimlari o'rtasida SAN kommutatorlari;

zaxira ma'lumotlarni qayta ishlash markazi (bosh ofis) va asosiy ma'lumotlarni qayta ishlash (Toshkent. sh MBXO) o'rtasidagi OTAL kabellari;

bank bankomatlarini protsessing markazlariga ulash uchun foydalaniladigan aloqa kanallari;

b) Bosh ofis va ABdagi lokal tarmoq, bankning MBXO, MBdagi lokal tarmoqlari, shu jumladan mahalliy tarmoqlarni tashkil qilish uchun foydalaniladigan kommutatorlar va kabellar;

9) Axborot resurslari:

a) Bank bosh ofisi va AB fayl serveri xodimlarining fayllarini saqlash uchun ushbu xodimlar tomonidan bosh ofis va AB binosida tashkil etilgan mahalliy tarmoq orqali kirish amalga oshiriladi, ushbu fayl serveri zaxira ma'lumotlarni qayta ishlash markazining server xonasida joylashgan;

b) Bankning har bir MBXO va BXMdagi fayl serverlari, ularning server xonalarida joylashgan bo‘lib, ular MBXO va BXM xodimlarining fayllarini saqlash uchun tashkil etilgan. MBXO va BXM xodimlarining ushbu fayl serverlariga kirishi MBXO va BXM lokal tarmoqlari orqali amalga oshiriladi;

c) Bank rasmiy sayti https://sqb.uz/, serveri “Unitel” MChJ xosting saytida joylashgan;

d) Bank internet-banking web-ilovalari https://ib.uzpsb.uz/ (jismoniy shaxslar uchun) va https://clbank.uzpsb.uz/ (yuridik shaxslar uchun), serverlari asosiy ma’lumotlarni qayta ishlash markazi server xonasida joylashgan. Bank mijozlarini ulash va ularga interaktiv xizmatlarini ko‘rsatish uchun internet tarmog‘iga ulangan;

e) Bank mobil banking bo‘yicha web-ilovalar, serverlari bank asosiy ma’lumotlarni qayta ishlash markazining server xonasida joylashgan jismoniy va yuridik shaxslar uchun alohida, bankning mobil mijozlarini Joyda mobil ilovalari (jismoniy shaxslar uchun) orqali ulash va SQB -Biznes (yuridik shaxslar uchun) va ularga interaktiv xizmatlarini ko'rsatish uchun internetga ulangan;

f) Bankning ichki web-sayti serveri bankning asosiy ma’lumotlarni qayta ishlash markazida joylashgan va bank xodimlari korporativ tarmoq orqali ulangan;

g) axborot tizimlarining ma’lumotlar bazalari, shu jumladan bankning ABT ma’lumotlar bazasi, ularning elektron arxivlari.

10) Himoyalangan axborotni tashuvchilar, shu jumladan axborotni kalitini tashuvchilar – elektron raqamli imzo kriptografik kalitlarini (keyingi o‘rinlarda – ERI deb yuritiladi) tashuvchilar;

11) Himoyalangan xonalar:

Toshkent shahridagi MBXO binosidagi asosiy ma’lumotlarni qayta ishlash markazi (manzil, Toshkent sh., Mustaqillik ko‘chasi, 5-uy) va bosh ofis binosidagi zaxira ma’lumotlarni qayta ishlash markazi (manzil, Toshkent sh., Shahrisabz ko‘chasi, 3-uy) va ularning xonalarida.

AB, MBXO ва BXMdagi kassa uzellari xonalari;

korporativ tarmoqqa, fayl serveriga, virusga qarshi serverga (faqat MBXO-da) va lokal tarmoq uchun tarmoq uskunalariga ulanish uchun marshrutizatorlar yoki

modemlar joylashgan MBXO va BXM server xonalari);

bankning AB, MBXO ва BXMda konfidensial ma'lumotlarni qayta ishlash amalga oshiriladigan xonalar;

moddiy boyliklarni saqlash uchun xonalar (omborlar).

12) Axborotni himoya qilish vositalari (tarmoqlararo ekran, IDPS hujumlarini aniqlash va oldini olish vositalari, VPN tashkil qilish vositalari, virusga qarshi himoya vositalari, proksi-serverlar, AKH, DLP konfidensial ma'lumotlarning sizib chiqishini oldini olish tizimi va boshqalar).

13) Bankning ERI kalitlarini ro'yxatga olish markazi, ABT foydalanuvchilari bo'lgan bank xodimlari va internet-banking va mobil bankingdan foydalanuvchilari hamda bank mijozlari (faqat yuridik shaxslar) uchun ochiq ERI kalitlari sertifikatlarini va yopiq kalitlarni shakllantirishni ta'minlaydi.

14) Bankning axborot tizimlari;

15) Nomoddiy aktivlar (bank obro'si va imeji).

15. Bankda quyidagi axborot tizimlari tashkil etilgan:

1) Avtomatlashtirilgan bank tizimi (ABT) – bank mijozlari uchun to'lovlarini amalga oshirish tizimi.

ABT quyidagi apparat va dasturiy ta'minot kompleksini o'z ichiga oladi:

ma'lumotlar bazasi serverlari (klaster rejimida ishlaydigan va asosiy ma'lumotlarni qayta ishlash markazida joylashgan ikkita ma'lumotlar bazasi serveri va zaxira ma'lumotlarni qayta ishlash markazida joylashgan bitta zaxira ma'lumotlar bazasi serveri);

bank korporativ tarmog'i orqali bank xodimlarining asosiy tizimiga kirishi uchun web-ilova serverlari (asosiy ma'lumotlarni qayta ishlash markazida joylashgan 4 ta ilova serveri).

2) asosiy ma'lumotlarni qayta ishlash markazida joylashgan va foydalanuvchilari bank mijozlari bo'lgan, internet tarmog'iga ulangan bank xizmatlarini ko'rsatish uchun internet-banking tizimi;

3) Joyda (jismoniy shaxslar uchun) va SQB-Bizness (yuridik shaxslar uchun) mobil banking tizimlari;

4) CRM mijozlar bilan munosabatlarni boshqarish tizimi (keyingi o'rinlarda CRM tizimi deb yuritiladi) serveri asosiy ma'lumotlarni qayta ishlash markazida joylashgan va foydalanuvchilari bank xodimlari hisoblanadi;

5) DWH korporativ ma'lumotlar ombori (keyingi o'rinlarda DWH tizimi deb yuritiladi) bank axborot tizimlaridan ma'lumotlarni yig'ish va kerakli tahliliy yoki hisobot ma'lumotlarini olish maqsadida ularni qayta ishlash uchun mo'ljallangan. DWH tizimining foydalanuvchilari bank xodimlari (menejerlari) hisoblanadi. DWH tizim serveri asosiy ma'lumotlarni qayta ishlash markazida joylashgan;

6) Bank CROBS (keyingi o'rinlarda CROBS tizimi) biznes-jarayonlari va vazifalarini avtomatlashtirish tizimi, ularning asosiy va zaxira ma'lumotlar bazasi hamda dastur serverlari asosiy ma'lumotlarni qayta ishlash markazida joylashgan. CROBS tizimi ABT tomonidan ko'zda tutilmagan funksional vazifalarni amalga oshirish uchun mo'ljallangan (ABT ni kengaytirish) va uning foydalanuvchilari bank xodimlaridir;

7) ELMA BPM biznes-jarayonlarini boshqarish tizimi (keyingi o'rinlarda

ELMA BPM tizimi) tovar va xizmatlarni chakana sotishda kredit konveyeri funksiyasiga ega bo'lgan, jismoniy shaxslarga xizmat ko'rsatish jarayonlarini avtomatlashtirish uchun mo'ljallangan. ELMA BPM tizim serveri asosiy ma'lumotlarni qayta ishlash markazida joylashgan. Ushbu tizim foydalanuvchilari bank xodimlaridir;

8) SAP BPC va SAP PaPm tizimi (keyingi o'rinlarda SAP tizimi deb yuritiladi) resurslarni rejalashtirish va biznes jarayonlari tizimi asosida ERP sinfini byudjetlashtirish va narxlash. SAP tizimining foydalanuvchilari bank xodimlaridir. SAP tizimining ma'lumotlar bazasi va ilova serverlari asosiy ma'lumotlarni qayta ishlash markazida joylashgan;

9) Bankda valyuta operatsiyalari va xalqaro to'lovlarni amalga oshirish uchun banklar o'rtasida moliyaviy xabarlarni o'tkazishga mo'ljallangan SWIFT tizimi/ (bundan buyon matnda SWIFT tizimi deb yuritiladi). Bankda SWIFT tizimi alohida asosiy va zaxira serverda tashkil etilgan zaxira ma'lumotlarni qayta ishlash markazi server xonasida joylashgan;

10) VISA, Mastercard, UnionPay, JSB va boshqalar xalqaro plastik kartochkalari protsessing tizimi xalqaro plastik kartalarni faollashtirish va boshqarish hamda bank xodimlari va mijozlarning ushbu kartalar bo'yicha so'rovlarini ko'rib chiqish uchun mo'ljallangan. bank xalqaro plastik kartochkalarini protsessing tizimi Way4 protsessing platformasi (keyingi o'rinlarda Way4 xalqaro plastik kartochkalarini protsessing tizimi deb yuritiladi) negizida qurilgan bo'lib, asosiy ma'lumotlarni qayta ishlash markazi server xonasida joylashgan, zaxira serverlari esa – zaxira ma'lumotlarni qayta ishlash markazida joylashgan.

16. Bundan tashqari, bankda quyidagilar tashkil etilgan:

1) Bank Call-markazidagi bankning mijozlar qo'ng'iroqlarini qayta ishlash tizimining serveri. Smiddle dasturiy ta'minoti asosida qurilgan, shuningdek, ilovalarni birlashtirish va qayta ishlash tizimini tashkil qilish uchun Redmine dasturidan foydalangan holda qurilgan;

2) Xalqaro pul o'tkazmalari tizimlari, xususan: Zolotaya Korona, RIA, Western Union, Contact, Unistream, MoneyGram va boshqalar asosiy ma'lumotlarni qayta ishlash markazida joylashgan.

17. Bank quyidagi tashqi axborot tizimlari bilan o'zaro hamkorlik qiladi (ma'lumotlar almashadi):

O'zbekiston Respublikasi Markaziy bankining tashqi bank axborot tizimlari;

UzCard va HUMO tashqi protsessing tizimlari;

CRIF kredit axborot xizmati tizimi;

O'zbekiston Respublikasi banklar assotsiatsiyasi kredit byurosining kredit axborot-tahlil markazi (ASOKI);

Davlat soliq qo'mitasi tizimi;

O'zbekiston Respublikasi Bosh prokuraturasi Majburiy ijro byurosi tizimi;

Pensiya jamg'armasi tizimi (Xalq banki) va boshqalar.

Shuningdek, bankning ichki tizimlar bilan o'zaro hamkorlik qiladi:

Bank internet-banking va mobil banking tizimlari;

18. O'z DSt 2814:2014 "Axborot texnologiyalari. Avtomatlashtirilgan tizimlar. Ma'lumotlarga ruxsatsiz kirishdan himoya qilish darajasi bo'yicha tasniflash"

davlat standarti talablariga asosan bank “ABT Colvir” axborot tizimi 1B xavfsizlik sinfiga kiradi.

19. Bank axborot tizimlarining xavfsizlik darajasi bo‘yicha tasniflash Davlat va xo‘jalik boshqaruvi organlari, mahalliy davlat hokimiyati organlarining axborot xavfsizligini ta’minlashga oid talablarga muvofiq amalga oshirildi (O‘zbekiston Respublikasi Axborot-kommunikatsiya xavfsizligi bo‘yicha texnik kengashning 2017 yil 17 noyabrdagi 7-son bayonnomasiga 2-ilovasi) va 1-jadvalda ko‘rsatilgan.

20. Bank axborot resurslarining xavfsizlik darajasi bo‘yicha tasnifi mazkur siyosatga 13-ilovaga muvofiq bank axborot resurslari reyestrida keltirilgan.

1- Jadval

Bank axborot tizimlarining xavfsizlik darajasi bo‘yicha tasnifi.

Axborot tizimi nomi	Axborot tizimi masshtabi	Qayta ishlanadigan axborot toifasi	Axborot tizimi ahamiyatlilik darajasi	Axborot tizimi himoyalanganlik sinfi*
Internet-Banking va mobil Banking tizimlari	Sohaga tegishli Respublika miqyosida	Barcha uchun konfidensial	Yuqori	IS4
CRM tizimi	Sohaga tegishli Respublika miqyosida	Konfidensial axborot	Yuqori	IS4
DWH tizimi	Sohaga tegishli Respublika miqyosida	Konfidensial axborot	O’rta	IS3
CROBS tizimi	Sohaga tegishli Respublika miqyosida	Konfidensial axborot	Yuqori	IS3
ELMA BPM tizimi	Sohaga tegishli Respublika miqyosida	Konfidensial axborot	Yuqori	IS2
SAP tizimi	Sohaga tegishli Respublika miqyosida	Konfidensial axborot	O’rta	IS3
EHAT tizimi	Sohaga tegishli Respublika miqyosida	Konfidensial axborot	O’rta	IS2
SWIFT tizimi	Sohaga tegishli Respublika miqyosida	Konfidensial axborot	Yuqori	IS4
Way4 Prosessing tizimi	Sohaga tegishli Respublika miqyosida	Konfidensial axborot	Yuqori	IS4

** Izoh: Eng past xavfsizlik klassi birinchi sinf (IS1), eng yuqori darajasi - to’rtinchi sinf (IS4)*

VI. Axborot xavfsizligi xavf ehtimolligi va tahdidlarning modeli

21. Bankning axborot xavfsizligiga tahdid modeli har bir muhim va muhim

himoya obyekti uchun belgilaydi va quyidagilarni o‘z ichiga oladi:

himoyalangan obyektning tavsifi;

himoyalangan obyektga xavfsizlikka mumkin bo'lgan tahdidlarining ro'yxati va tavsifi;

buzg'unchi modeli;

mumkin bo'lgan zaifliklar;

tahdidlarni amalga oshirish usuli;

tahdidlarni amalga oshirish oqibatlari.

22. Bank da axborot xavfsizligiga tahdidlar modeliga ta’sir qilish usuli bo‘yicha quyidagi asosiy tahdidlar kiradi:

kompyuter tahdidlari;

fizik tahdidlar;

texnik kanallardan foydalangan holda tahdidlar;

texnogen tahdidlar, shu jumladan tabiiy tahdidlar.

23. Kompyuter-texnik tahdidlar himoya obyekti va/yoki dasturlardan, kompyuter vositalaridan, shuningdek ulardagi zaifliklardan foydalangan holda tarmoqning o‘zaro ta’siri orqali amalga oshiriladi. Kompyuter tahdidlariga texnik nosozliklar ham kiradi.

24. Ta’sir xususiyati bo‘yicha kompyuter-texnik tahdidlar quyidagilarga bo‘linadi:

axborot bank faoliyatiga zid, nomaqbul, elektron shaklda axborotni, shuningdek shaxsiy va maxfiy moliyaviy ma’lumotlarni o‘g‘irlashga qaratilgan nomaqbul kontentni (fishing) tarqatish;

dasturiy ta’minot - zararli dastur, ixtisoslashtirilgan dasturlardan foydalanish yoki dasturlarda e’lon qilinmagan funksional imkoniyatlar (zakladkalar) foydalanish;

tarmoq - tarmoqdagi zaifliklarni, tarmoq protokollari, dasturlari va vositalarini ishlatadigan, shuningdek ma'lumotlarni o'g'irlash, yo'q qilish yoki o'zgartirish, noqonuniy harakatlar qilish uchun ruxsatsiz kirishni olishga qaratilgan axborot uzatish kanallari va maxsus dasturiy vositalardan foydalanadigan tarmoq hujumlari va ta'siri; normal faoliyatni buzish;

apparat va dasturiy ta'minotga texnik xizmat ko'rsatishni rad etish – ishlamay qolishi yoki texnik xizmat ko'rsatuvchi xodimlarning xatolari yoki qoidabuzarning unga ta'siri tufayli ishlamay qolishi.

25. Jismoniy tahdidlar jismoniy kirish, buzg‘unchining himoya obyektiga jismoniy ta’siri orqali amalga oshiriladi;

Jismoniy tahdidlar quyidagilarga yo‘naltirilishi mumkin:

o‘chirib yuborish yoki yo‘q qilish;

ishdan chiqarish yoki zarar yetkazish;

noqonuniy operatsiyalar;

o‘g‘irlash.

Shuningdek, axborotlashtirish obyektiga va/yoki axborotga to‘g‘ridan-to‘g‘ri kirish orqali olingan konfidensial ma’lumotlarning tarqalishini o‘z ichiga oladi.

26. Texnik kanallardan foydalanadigan tahdidlar asosan ma’lumotlarning tarqalishiga qaratilgan va texnik vositalar va aloqa kanallariga ta’sir qilish va to‘sish uchun ham ishlatilishi mumkin. Ma’lumotlar sizib chiqish kanallari sifatida quyidagilar qo‘llaniladi: elektromagnit signallar, shu jumladan soxta elektromagnit

nurlanish va texnik vositalar va aloqa kanallarining aralashuvi, akustik va vibratsiyali signallar, elektr signallari va radionurlanishlar, ko‘zga ko‘rinadigan, infraqizil va ultrabinafsha nurlanishlaridagi optik (televizion, foto va vizual) signallar.

27. Texnogen tahdidlarga yong‘inlar, portlashlar, inshootlarning qulashi, suv toshqini va boshqalar, shu jumladan, tabiiy ofatlar natijasida vayron bo‘lishi yoki ishdan chiqishi shuningdek Bankning axborot-kommunikatsiya infratuzilmasiga zarar yetkazishi mumkin bo‘lgan xavflar kiradi.

28. Bank axborot xavfsizligiga tahdidlar yuzaga kelish xususiyatiga ko‘ra tabiiy (obyektiv) va sun’iy (subyektiv) bo‘lishi mumkin.

29. Axborot xavfsizligiga tahdidlar manbalari ichki bank ichidagi tahdidlar manbai) va tashqi Bankdan tashqaridagi tahdidlar manbai) bo‘lishi mumkin.

30. Har bir himoya obyekti uchun axborot xavfsizligiga tahdidlarning qanchalik muhimligini aniqlash uchun ikkita mezon qo‘llaniladi:

tahdid xavfi;

tahdidlarning paydo bo‘lishi va ularni amalga oshirish imkoniyati.

Tahdidning xavfi tahdid natijasida kelib chiqadigan oqibatlarga qarab baholanadi:

yuqori - kuchli darajali tahdidlar;

o‘rtacha – o‘rtacha darajali tahdidlar;

past – past darajadagi tahdidlar.

Tahdidning paydo bo‘lishi va uni amalga oshirish imkoniyati quyidagi ma’nolarga ega:

yuqori - zaiflik mavjudligi va tahdidlardan himoya qilish usullari va vositalari mavjud emasligi, axborot makonida tahdidlarning tarqalishi;

o‘rta - dasturiy ta’minotda zaifliklar mavjudligi, axborotni himoya qilishning kam samarali usullari va vositalaridan foydalanish, tahdid axborot makonida keng tarqalmaganligi;

past - zaiflikning mavjud emasligi, himoya vositalaridan foydalanish.

Axborot xavfsizligiga tahdidning dolzarbligi 1-jadvalda keltirilgan quyidagi qoidalarga muvofiq belgilanadi.

1-jadvalda

Axborot xavfsizligi tahdidlarini aniqlash tartibi

Tahdidni amalga oshirish imkoniyati	Tahdidlarning xavfliligi		
	Past	O‘rta	Yuqori
Past	-	-	Aktual
O‘rta	-	Aktual	Aktual
Yuqori	Aktual	Aktual	Aktual

31. Bank axborot xavfsizligiga tahdidlar modeli himoya qilish obyektlariga nisbatan belgilanadi va quyidagilarni o‘z ichiga oladi:

tahdidning tavsifi;

tahdid manbai va mohiyati;

tahdidlarni amalga oshirish usuli;

foydalanilgan zaifliklar;

ta’sir obyektlari;

tahdidning dolzarbligi (xavf va amalga oshirish imkoniyati);

Bankning axborot xavfsizligiga asosiy tahdidlar modeli 2-jadvalda keltirilgan.

32. Bankda xavflarni tahlil qilish va baholash O‘z DSt ISO/IEC 27005:2013 “Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish tizimini joriy qilish bo’yicha ko’rsatmalar” davlat standartiga muvofiq amalga oshiriladi.

33. Xatarlarni identifikatsiyalash natijalari qo'llanma bo'lib xizmat qiladi, tegishli boshqaruv harakatlarini va axborot xavfsizligini boshqarish ustuvorliklarini belgilaydi shuningdek, ushbu xavflardan himoya qilish uchun tanlangan chora-tadbirlar, usullar va vositalarni amalga oshirishga yo'naltirilishi kerak.

34. Xatarlarni identifikatsiya qilish xavflarni miqdoriy yoki sifat jihatidan baholashning tizimli yondashuvini (xavfni tahlil qilish) va xavflarning ahamiyatini aniqlash uchun baholangan xavflarni xavf mezonlari bilan taqqoslash jarayonini o'z ichiga oladi.

Xatarlarni identifikatsiya qilishdan tashqari, risklarni boshqarish jarayonlari quyidagilarni o'z ichiga olishi kerak: xavfni bartaraf qilish, xavfni qabul qilish, xavflarni monitoring qilish va ko'rib chiqish.

35. Bankda risklarni tahlil qilish va baholash mas’ul departament tomonidan amalga oshiriladi.

36. Bank faoliyati uchun quyidagi asosiy xavflar mavjud:

qoidabuzarlar tomonidan (o'chirish, yo'q qilish yoki o'g'irlash) tizimlarga ruxsatsiz kirish, zararli dasturlarga ta'sir qilish, tarmoq hujumlari amalga oshirish, xodim xatolari yoki dastur xatolari, texnik nosozliklar natijasida himoyalangan obyektlarning noto'g'ri ishlashi.

himoyalangan ma'lumotlarning konfidensiallik va yaxlitligini buzish, noto'g'ri va qarama-qarshi ma'lumotlarni tarqatish;

noqonuniy xatti-harakatlar va noqonuniy moliyaviy operatsiyalarni amalga oshirish, moliyaviy firibgarlik.

37. Ushbu xavflarning quyidagi oqibatlari:

bank xizmatlarini ko'rsatishni to'xtatib turish yoki ularni xizmat ko'rsatishning sifat pastligi;

bank faoliyatining uzluksizligini buzish, u tomonidan alohida vazifalarni bajarish yoki alohida axborot texnologiyalarni ishlab chiqarish jarayonlarini joriy etish uzluksizligini buzish;

bankning moliyaviy yo'qotishlar;

bank tijorat siri, bank, shaxsga doir sirlarni va boshqa konfidensial ma'lumotlarni oshkor qilish;

bank mijozlarga ma’naviy va moddiy (moliyaviy yo‘qotishlar) yetkazish;

bank imiji va obro‘siga putur yetkazish.

38. Xatarlarni tahlil qilishda faqat axborot xavfsizligiga tahdidlarning aktualligi hisobga olinadi.

Himoya obyektlariga nisbatan axborot xavfsizligi uchun xavf va tahdidlarning tahlili 3-jadvalda keltirilgan.

39. Xavflarni baholash uchun quyidagi shkala ishlatilgan:

yuqori – 6-8;

o‘rta – 3-5;

past – 0-2.

Bank uchun himoya qilish obyektining qiymati (ahamiyati) 0 dan 10 gacha bo‘lgan shkala bo‘yicha baholandi.

2-jadval.

Bankni axborot xavfsizligiga asosiy tahdidlar modeli

Tahdidlar nomi	Manbasi va mohiyati	Amalga oshirish usuli	Foydalanilgan zaifliklar	Ta'sir obyektlari	Xavflilik darajasi	Amalga oshirish imkoniyati	Aktualligi
1. Kompyuter-texnik tahdidlar							
Ma'lumot	Manbasi: ichki va tashqi Xususiyati: subyektiv	Shaxsga doir ma'lumot, konfidensial va moliyaviy ma'lumotlarni o'g'irlashga qaratilgan (fishing), shuningdek, noto'g'ri va bankning faoliyatiga zid bo'lgan ma'lumotlarni elektron shaklda tarqatish	Mijoz ishonchi	bank obro'si va imiji, Konfidensial axborot, bank mijozlari	O'rta	O'rta	Aktual
Dasturiy ta'minot	Manbasi: ichki va tashqi Xususiyati: subyektiv	Zararli dasturlar, maxsus dasturlar (josuslik dasturlari) yoki dasturlarda e'lon qilinmagan funksiyalar (zakladkalar)	Davriy yangilanmagan va litsenziyaga ega bo'lmagan antivirus dasturi, Operatsion tizim va dasturiy ta'minot zaifliklari	Bankning elektron shakldagi ma'lumotlari (ma'lumotlari), amaliy va tizim dasturlari, ma'lumotlarni qayta ishlash, saqlash va uzatish vositalari, LHT, korporativ tarmoq, bank web-resurslari, axborot tizimlarining ma'lumotlar bazalari, axborotni himoya qilish vositalari.	Yuqori	O'rta	Aktual

Tarmoq	Manbasi: ichki va tashqi Xususiyati: subyektiv	Axborotni o'g'irlash, yo'q qilish yoki o'zgartirish, noqonuniy xatti-harakatlar qilish, normal ishlashini buzish uchun ruxsatsiz kirishni amalga oshirishga qaratilgan axborot uzatish kanallari va maxsus dasturiy vositalardan foydalangan holda tarmoq hujumlari	Tarmoq, tarmoq protokollari, dasturlar va vositalarning zaifliklari	Bankning elektron shakldagi ma'lumotlari (ma'lumotlari), amaliy va tizim dasturlari, ma'lumotlarni qayta ishlash, saqlash va uzatish vositalari, mahalliy tarmoq, korporativ tarmoq, Bankning web-resurslari, ma'lumotlar bazalari va axborot tizimlari, axborotni himoya qilish vositalari.	Yuqori	Yuqori	Aktual
Ishlamay qolishi yoki funksional buzilish	Manbasi: ichki va tashqi Xususiyati: subyektiv va obyektiv	Ma'nan eskirganligi yoki dasturning xatoliklari, shuningdek, mas'ul xodimning xatolari tufayli ishlamay qolishi	Texnik va dasturiy vositalar va ishlash jarayonidagi zaifliklar	Dasturiy ta'minotlar, ma'lumotlarni qayta ishlash, saqlash va uzatish vositalari, ma'lumotlarni himoyalash vositalari	Yuqori	O'rta	Aktual
2. Jismoniy tahdidlar	Manbasi: ichki va tashqi Xususiyati: subyektiv	Himoyalangan obyektga jismoniy ta'sir o'tkazish (ta'sir qilish) orqali buzilish yoki yo'q qilish, zarar yetkazish, noqonuniy operatsiyalarni amalga oshirishga qaratilgan ishlar jismoniy kirish orqali	Jismoniy himoya qilish vositalaridagi zaifliklar	Bankning elektron ko'rinishidagi ma'lumotlari, hujjatlashtirilgan ma'lumotlar, axborot tashish qurilmalari, aloqa kanallari,	Yuqori	O'rta	Aktual

		amalga oshiriladi.		ma’lumotlarni qayta ishlash, saqlash va uzatishning texnik vositalari shuningdek, ularning dasturiy ta’minoti, binolari, shkaflari va seyflari, boshqa moddiy boyliklari			
3. Ma’lumot chiqib ketish texnik kanali orqali kelib chiqadigan tahdidlar	Manbasi: ichki va tashqi Xususiyati: subyektiv	Ma’lumotlar chiqib ketishining texnik kanallaridan foydalanish: elektromagnit signallar, shu jumladan elektromagnit nurlanish va texnik uskunalar, aloqa kanallarining shovqinlari, akustik va vibroakustik signallar, elektr signallari va radiosignallar, optik (televizion, fotografik va vizual) signallar infraqizil va ultrabinafsha diapazonlarida ko’rinadigan to’lqinlar	Ma’lumot chiqib ketish texnik kanali mavjudligi	Elektron ko’rinishidagi ma’lumotlar, ma’lumotlarni qayta ishlash, saqlash va uzatishning texnik vositalari va aloqa kanallari	O’rta	Past	Aktual emas
4 Texnogen tahdidlar	Manbasi: ichki va tashqi Xususiyati: subyektiv va obyektiv	Yong’inlar, portlashlar, inshootlarning qulashi, suv toshqini va boshqa tabiiy ofatlar	Yong'in xavfsizligi va mehnatni muhofaza qilish talablarini buzish	Barcha himoya obyektlari	Yuqori	Past	Aktual

3-jadval.

Bankning himoya qilish obyektlariga nisbatan axborot xavfsizligi risklarini tahlil qilish va baholash natijasi

№	Aktual tahdidlarning nomi	Tahdid ehtimoli	Oqibatlari	Ko'rilgan choralar	Xavfni baholash
1.	Bank axborot tizimlarining axborotni qayta ishlash va saqlash vositalari (MB serverlar va amaliy va ma'lumotlarni saqlash tizimlari) hamda ularda foydalaniladigan dasturiy ta'minot (operatsion tizim, MBBT, amaliy dasturlar va amaliy dasturlar): Qiymati (ahamiyati) - 10				
1.1	Zararli dastur bilan zararlash	0,6	Normal ishlashning buzilishi, tizimning to'liq ishdan chiqishi	Antivirus vositalaridan foydalanish	6 (yuqori)
1.2	Xizmatni rad etish	0,8	Normal ishlashning buzilishi, muayyan texnologik vazifalarni bajarmaslik, tizimning to'liq ishdan chiqishi	Serverlar, ma'lumotlarni saqlash tizimlari va ma'lumotlarning saqlanganligi	6 (yuqori)
1.3	Normal ishlashni buzishga qaratilgan tarmoq hujumlari (DoS, DDoS hujumlari)	0,7	Normal ishlashning buzilishi, tizimning to'liq ishdan chiqishi	IDPSni qo'llash	7 (yuqori)
1.4	Ruxsatsiz kirishga qaratilgan tarmoq hujumlari	07	Normal ishlashning buzilishi, ma'lumotlarga kirish (konfidensial yoki yaxlitlikni buzish, o'zgartirish) yoki obyektlarga (boshqaruv nazorati, konfiguratsiyani o'zgartirish)	IDPS va tarmoqlararo ekranni qo'llash	7 (yuqori)
1.5	Ruxsatsiz jismoniy kirish	0,4	Normal ishlashni buzish, ma'lumotlarga kirish (konfidensial yoki yaxlitlikni buzish) yoki obyektlarga kirish (boshqaruv nazorati, konfiguratsiyani o'zgartirish)	ma'lumotlarni qayta ishlash markazi server xonalariga kirishni cheklash	3 (o'rta)
1.6	Texnogen tahdidlar va tabiiy ofatlar (favqulodda vaziyatlar)	0,2	Xonadagi obyektlar va ma'lumotlarning yo'qolishi	zaxira ma'lumotlarni qayta ishlash	2 (past)

			(moliyaviy yo'qotish), noto'g'ri ishlash	markazidan foydalanish	
2.	Axborotni qayta ishlash vositalari (serverlari) va ularda foydalaniladigan dasturiy ta'minot (operatsion tizim, ilovalar va amaliy dasturlar) axborot tizimlari va resurslari: Internet-Banking va mobil Banking, CRM tizimi, DWH tizimi, CROBS tizimi, SAP tizimi, ELMA BPM tizimi, xalqaro plastik kartalarni qayta ishlash tizimi Way4 Qiymati (ahamiyati) - 8				
2.1	Zararli dastur tarqalishi	0,6	Normal ishlashning buzilishi, tizimning to'liq ishdan chiqishi	Antivirus vositalaridan foydalanish	6 (yuqori)
2.2	Xizmatni rad etish	0,8	Normal ishlashning buzilishi, muayyan texnologik vazifalarni bajarmaslik, tizimning to'liq ishdan chiqishi	Serverlar va ma'lumotlarni zaxiralash	7 (yuqori)
2.3	Normal ishlashni buzishga qaratilgan tarmoq hujumlari (DoS, DDoS hujumlari)	0,7	Normal ishlashning buzilishi, tizimning to'liq ishdan chiqishi	IDPSni qo'llash	6 (yuqori)
2.4	Ruxsatsiz kirishga qaratilgan tarmoq hujumlari	07	Ruxsatsiz kirishga yo'naltirilgan tarmoq hujumlari normal ishlashni buzish, ma'lumotlarga kirish (konfidensial yoki yaxlitlikni buzish, o'zgartirish) yoki obyektlarga (boshqaruvni boshqarish, konfiguratsiyani o'zgartirish)	IDPS va tarmoqlararo ekranni qo'llash	6 (yuqori)
2.5	Ruxsatsiz jismoniy kirish	0,4	Normal ishlashni buzish, ma'lumotlarga kirish (konfidensiallik yoki yaxlitlikni buzish) yoki obyektlarga kirish (boshqaruv nazorati, konfiguratsiyani o'zgartirish)	Server xonasiga kirishni cheklash	3 (o’rta)
2.6	Texnogen tahdidlar va tabiiy ofatlar (favqulodda vaziyatlar)	0,2	Xonadagi obyektlar va ma'lumotlarning yo'qolishi (moliyaviy yo'qotish), noto'g'ri ishlash	Zaxira ma'lumotlarni qayta ishlash markazi resurslarini jalb qilish	3 (o’rta)

3.	Axborotni qayta ishlash vositalari (serverlari) va ularda foydalaniladigan dasturiy ta'minot (operatsion tizim, ilovalar va amaliy dasturlar) axborot resurslari va korporativ elektron pochta, IP telefoniya, korporativ messenjer, fayl serveri, rasmiy web-sayt, ichki web-sayt intranet. Qiymati (ahamiyati) - 7				
3.1	Zararli dastur tarqalishi	0,6	Normal ishlashning buzilishi, tizimning to'liq ishdan chiqishi	Antivirus vositalaridan foydalanish	6 (yuqori)
3.2	Xizmatni rad etish	0,8	Normal ishlashning buzilishi, muayyan texnologik vazifalarni bajarmaslik, tizimning to'liq ishdan chiqishi	Serverlar va ma'lumotlarni zaxiralash	5 (yuqori)
3.3	Normal ishlashni buzishga qaratilgan tarmoq hujumlari (DoS, DDoS hujumlari)	0,7	Normal ishlashning buzilishi, tizimning to'liq ishdan chiqishi	IDPSni qo'llash	6 (yuqori)
3.4	Ruxsatsiz kirishga qaratilgan tarmoq hujumlari	07	Ruxsatsiz kirishga yo'naltirilgan tarmoq hujumlari normal ishlashni buzish, ma'lumotlarga kirish (konfidensial yoki yaxlitlikni buzish, o'zgartirish) yoki obyektlarga (boshqaruvni boshqarish, konfiguratsiyani o'zgartirish)	IDPS va tarmoqlararo ekranni qo'llash	6 (yuqori)
3.5	Ruxsatsiz jismoniy kirish	0,4	Normal ishlashni buzish, ma'lumotlarga kirish (konfidensiallik yoki yaxlitlikni buzish) yoki obyektlarga kirish (boshqaruv nazorati, konfiguratsiyani o'zgartirish)	Ma'lumotlarni qayta ishlash markazining server xonalariga va MBXO va BXM server xonalariga kirishni cheklash	3 (o’rta)
3.6	Texnogen tahdidlar va tabiiy ofatlar (favqulodda vaziyatlar)	0,2	Xonadagi obyektlar va ma'lumotlarning yo'qolishi (moliyaviy yo'qotish), noto'g'ri ishlash	Zaxira ma'lumotlarni qayta ishlash markazi resurslarini jalb qilish	3 (o’rta)
4.	Tarmoq uskunalari (yadro kommutatorlar, marshrutizatorlar) va korporativ tarmoq aloqa kanallari Qiymati (ahamiyati) - 8				
4.1	Tarmoq uskunasiga xizmat ko'rsatishni	0,6	Normal faoliyatni buzish, bir yoki	Tarmoq uskunasining	6

	rad etish		barcha yo'nalishlarda aloqani yo'qotish	zaxiralash	(yuqori)
4.2	Aloqa kanalining uzilishi	0,5	Yo'nalishdagi aloqani yo'qotish yoki Internetga kirish yoki tashqi axborot tizimlari bilan o'zaro ta'sir qilish	Aloqa kanallarini zaxiralash	4 (o'rta)
4.3	Normal ishlashni buzishga qaratilgan tarmoq hujumlari (DoS, DDoS hujumlari)	0,7	Normal ishlashning buzilishi, vositalarning to'liq ishdan chiqishi	IDPSni qo'llash	6 (yuqori)
4.4	Ruxsatsiz kirishga qaratilgan tarmoq hujumlari	07	Normal ishlashni buzish, vositalarga (boshqaruv nazorati, sozlamalarga o'zgartirishlar kiritish)	IDPS va tarmoqlararo ekranni qo'llash,	6 (yuqori)
4.5	Ruxsatsiz jismoniy kirish	0,4	Normal ishlashning buzilishi, obyektlarga kirish (boshqaruv nazorati, sozlash o'zgarishlari)	Ma'lumotlarni qayta ishlash markazining server xonalariga kirishni cheklash	3 (o'rta)
4.6	Texnik kanallaridan foydalangan holda tahdidlar axborot sizib chiqishi	0,3	Axborotning tarqalishi, texnik vositalar va aloqa kanallarining ta'siri va bostirilishi	Himoya vositalari va kanallarini xavfsiz joylashtirish choralari	2 (past)
4.7	Texnogen tahdidlar va tabiiy ofatlar (favqulodda vaziyatlar)	0,2	Xonadagi vositalarni yo'qotilishi (moliyaviy yo'qotish), noto'g'ri ishlash	Zaxira ma'lumotlar qayta ishlash markazining tarmoq uskunasini faollashtirish	3 (o'rta)
5.	Bank Bosh ofisi, MBXO, BXM lokal tarmoqlarining tarmoq uskunalari (kamutatorlari) va aloqa kanallari. Qiymati (ahamiyati) - 5				
5.1	Tarmoq uskunasiga xizmat ko'rsatishni rad etish	0,6	Normal ishlashning buzilishi, bir yoki bir nechta ish stansiyalari va serverlar uchun aloqa yo'qolishi	Qo'shimcha tarmoq uskunalarini jalb qilish	5 (o'rta)
5.2	Kabelning buzilishi	0,4	Bir yoki bir nechta ish stansiyalari va serverlar uchun aloqa yo'qolishi	Kabelni qayta tiklash	5 (o'rta)
5.3	Ruxsatsiz jismoniy kirish	0,4	Normal faoliyatni buzilishi	Xonalarga shkaflarni joylashtirish	3 (o'rta)

5.4	Texnik kanallaridan foydalangan holda tahdidlar axborot sizib chiqishi	0,3	Axborotning tarqalishi, texnik vositalar va aloqa kanallarining ta'siri va bostirilishi	Himoya vositalari va kanallarini xavfsiz joylashtirish choralari	2 (past)
5.5	Texnogen tahdidlar va tabiiy ofatlar (favqulodda vaziyatlar)	0,2	Xonadagi vositalarni yo'qotilishi (moliyaviy yo'qotish), noto'g'ri ishlash	Qo'shimcha kommutatorlarni tiklash yoki ishlatish	3 (o'rta)
6.	**Xodimlarning ish stansiyalari va ularga o'rnatilgan dasturiy ta'minot (operatsion tizim va amaliy dasturlar) Qiymati (ahamiyati) - 4**				
6.1	Zararli dastur tarqalishi	0,6	Normal ishlashning buzilishi, to'liq ishlamay qolishi, ma'lumotlarning yo'qolishi	Antivirus vositalaridan foydalanish	4 (o'rta)
6.2	Ish stansiyasi, uning komponenti yoki dasturiy ta'minotiga xizmat ko'rsatishni rad etish	0,6	Normal faoliyatni buzish, ma'lumotni yo'qotish	Disklardagi ma'lumotlarning zaxiralash, profilaktika qilish	4 (o'rta)
6.3	Ruxsatsiz jismoniy kirish	0,4	Axborotning normal ishlashini buzish, sizib chiqish yoki yo'q qilish	Parolni o'rnatish, tashrif buyuruvchilarning harakatlarini kuzatish	3 (o'rta)
6.4	Texnik kanallaridan foydalangan holda tahdidlar axborot sizib chiqishi	0,2	Axborotni chiqib ketishi	Nazorat qilinadigan hududga joylashtirish	1 (past)
6.5.	Texnogen tahdidlar va tabiiy ofatlar (favqulodda vaziyatlar)	0,2	Xonadagi vositalarni yo'qotilishi (moliyaviy yo'qotish), noto'g'ri ishlash	Zaxira ish stansiyalarini foydalanish yoki ularni tiklash	2 (past)
7.	**Konfidensial ma'lumotlar Qiymati (ahamiyati) - 7**				
7.1	Ruxsatsiz jismoniy kirish	0,5	Axborotning konfidensialligini buzish	Seyflarga joylashtirish va nazorat qilish	6 (yuqori)
7.2	Xodim tomonidan aloqa kanallari (elektron pochta, messenjerlar, mobil telefonlar va boshqalar) orqali konfidensial ma'lumotlarning sizib	0,8	Axborotning chiqib ketishi (konfidensiallikni buzilishi).	Axborot chiqish kanallarini nazorat qilish, DLP tizimidan foydalanish	7 (yuqori)

	chiqishi.				
8.	**Bankomatlar, kiosklar, to'lov terminallari va elektron to'lov qurilmalari** **Qiymati (ahamiyati) - 7**				
8.1	Ruxsatsiz jismoniy kirish	0,7	Normal ishlashni buzilishi, nosozlik, o'g'irlik, xakerlik, ruxsatsiz harakatlar	kirish cheklangan yoki xavfsizlikka ega bo'lgan xonalarga joylashtirish, video kuzatuv tizimidan foydalanish	7 (yuqori)

4-jadval

Uchinchi tomon tashkilotlari bilan o'zaro aloqada axborot xavfsizligi xavfini tahlil qilish va baholash natijasi

Aktual tahdidlar	Oqibati	Xatar
Uchinchi tomon tashkilotlari bilan o'zaro hamkorlikda, ularning bank axborot tizimlari va resurslariga, axborotni qayta ishlash, saqlash va uzatish vositalariga hamda dasturiy ta'minotga (jismoniy kirish) kirishi.		
Ruxsatsiz jismoniy kirish huquqini olish	Normal ish faoliyatining buzilishi yoki vositaning boshqarilishini qo'lga kiritish, axborot qidirish moslamalarini o'rnatish yoki vositalarni o'zboshimchalik bilan boshqarish	5 (O'rta)
Axborotga ruxsatsiz jismoniy kirishni huquqini olish	Axborotning konfidensialligi va yaxlitligini buzilishi	4 (O'rta)
bank axborot tizimlarining uchinchi tomon tashkilotlari axborot tizimlari bilan ma'lumot almashish uchun shuningdek bank axborot tizimlaridan tashqi foydalanuvchilar bilan interaktiv bank xizmatlari ko'rsatishda o'zaro hamkorligi doirasida (mantiqiy kirish)		
Axborot tizimining vositalari va ma'lumotlariga tarmoqqa ruxsatsiz kirishni huquqini olish	normal ishlashini buzish holati, o'chirib qo'yish, ruxsatsiz boshqarish, ma'lumotlarning konfidensialligi, yaxlitligini buzish, uni blokirovka qilish va yo'qotish	6 (yuqori)
Zararli dasturlarni tarqatish	Normal faoliyatni buzish, ma'lumotni yo'qotish	6 (yuqori)

40. Uchinchi tomon tashkilotlari bilan o'zaro ma'lumot almashganda, shuningdek ular bankning axborot tizimlari va resurslariga kirishda yuzaga keladigan (yuzaga kelishi mumkin bo'lgan) axborot xavfsizligi xavfini tahlil qilish 4-jadvalda keltirilgan.

Uchinchi shaxslar bilan o'zaro ma'lumot almashganda axborotlarga bo'lgan xavflarni kamaytirish maqsadida siyosatning 11-bandida keltirilgan tashqi foydalanuvchilar bilan munosabatlar bandiga asosan xavfsizlik choralarini ko'rish lozim.

41. Axborot xavfsizligi xavfini boshqarish jarayoni nafaqat xavfni tahlil qilish va baholashni, balki axborot xavfsizligi xavfini kamaytirishga qaratilgan tadbirlarni ham o'z ichiga oladi.

Ushbu choralar "o'rta" va "yuqori" darajadagi xavflarga nisbatan qo'llanilishi kerak. Ushbu chora-tadbirlar Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan belgilanadi va bank rahbariyati bilan kelishiladi.

42. Axborot xavfsizligi xavflarni boshqarish bo'yicha ko'rilgan chora-tadbirlar natijalari hujjatlashtirilishi va ularning bajarilishi bank Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori tomonidan nazorat qilinishi kerak.

VII. Axborot xavfsizligi buzg‘unchisi modeli

43. Axborot xavfsizligi buzg’unchisi modeli subyektlarning imkoniyatlari va turlari, ruxsatsiz ta’sirlarning maqsadi to’g’risidagi ma’lumotlarni tizimlashtirish va ularga qarshi turishning yetarli darajada tegishli usullarini ishlab chiqish uchun shakllantiriladi. Buzg’unchi modelini ishlab chiqishda quyidagilar e’tiborga olinishi kerak:

buzg’unchilarning toifalari;

buzg’unchilarning xavflilik darajasi va ahamiyatini baholash va uning texnik imkoniyatlarini tahlil qilish xususiyatlari;

cheklov choralari va qarshi kurashish choralari.

44. Axborot xavfsizligini buzg’unchisi – atayin g’arazli niyat bilan (g’arazli manfaatlar asosida) yoki ularsiz (o’yin yoki o’zini ko’rsatish hamda boshqa maqsadlarda) buzishga qaratilgan taqiqlangan harakatlarni (operatsiyalarni) bajarishga uringan, shuningdek buning uchun turli xil imkoniyatlar, usul va vositalardan foydalangan shaxs.

45. Himoya obyektlariga nisbatan huquqbuzarliklarni xavfsizlik obyektlariga to’g’ridan-to’g’ri kirish huquqiga ega bo’lgan bank xodimlari, himoya qilish obyektlaridan foydalanish huquqiga ega bo’lmagan xodimlar va bankning xodimlari bo’lmagan shaxslar bo’lishi mumkin.

46. Buzg’unchilarning asosiy guruhlari va toifalari:

Buzg’unchilarni ko’rib chiqishda himoya qilish obyektlariga va shunga mos ravishda uning tarkibiy qismlariga ta’sir qilish imkoniyatlariga qarab guruhlarga bo’lish kerak. Buzg’unchilarning ikki guruhi mavjud:

1) tashqi buzg’unchilar - nazorat qilinadigan hududning ichki qismiga kirish huquqiga ega bo’lmagan va tegishli ravishda muhofaza qilinadigan obyekt va uning tarkibiy qismlariga bevosita ta’sir qilish imkoniga ega bo’lmagan shaxslar;

2) ichki buzg’unchilar - nazorat qilinadigan hududning ichki qismiga kirish huquqiga ega bo’lgan shaxslar va shunga mos ravishda himoya qilish obyektiga va uning qismlariga kirish huquqiga ega bo’lgan shaxslar.

Ichki potensial qoidabuzarlar - bankning axborotlashtirish obyektlari hududiga kirish huquqiga ega bo'lgan bank xodimlari.

47. Jahon o‘rtacha statistik ma’lumotlariga ko‘ra, Banklardagi tahdidlarning 82 foizi bevosita yoki bilvosita ishtirokida o‘z xodimlari tomonidan, 17 foizi tashqi tahdidlar va 1 foizi tasodifiy shaxslar tomonidan amalga oshiriladi.

Ushbu statistik ma’lumotlardan kelib chiqib, bank xodimlari va ularning noqonuniy xatti-harakatlarini nazorat qilish choralarini ko‘rish zarur. Xususan, bunday chora-tadbirlar quyidagilarni o'z ichiga oladi: shaxslarga axborot tizimlarida ishlashga yoki himoyalangan obyektlarga kirishga ruxsat berishning namunaviy modelini aniqlash, axborot tizimlarida xodimlarning harakatlarini hisobga olish, xodimlarning axborot tizimlariga kirishini cheklash (muayyan huquqlarni berish) va ushbu kirishni boshqarish, imtiyozli foydalanuvchilarni nazorat qilish, mumkin bo'lgan chiqish kanallarini kamaytirish, xodimlarni noqonuniy xatti-harakatlarning xavflari va oqibatlari to'g'risida xabardor qilish va boshqalar.

48. Yuqoridagi guruhlardan qat'iy nazar, buzg'unchilarni mumkin bo'lgan harakatlar orqali to'rtta sinfga ajratish mumkin:

birinchi (1-sinf) ma'lumotlarni qayta ishlash uchun oldindan belgilangan funksiyalar orqali vazifalarni boshlash bilan tavsiflanadi;

ikkinchi (2-sinf), birinchi darajali foydalanuvchilarning imkoniyatlarini o'z ichiga oladi va qo'shimcha ravishda yangi ma'lumotlarni qayta ishlash funksiyalari bilan o'z dasturlarini yaratish va ishlatish qobiliyatiga ega;

uchinchi (3-sinf) himoyalangan obyektning ishlashini boshqarish, ya'ni asosiy dasturiy ta'minotga, uning tarkibi va konfiguratsiyasiga ta'sir qilish qobiliyatiga ega;

to'rtinchi (4-sinf) himoya obyektlarining texnik jihozlarini loyihalashtirish, amalga oshirish va ta'mirlash bilan shug'ullanuvchi shaxslarning, shu jumladan himoya obyekti tarkibida ma'lumotlarni qayta ishlashning yangi funksiyalari bilan jihozlangan va dasturiy ta'minotni qamrab oluvchi imkoniyatlari bilan ajralib turadi.

49. Buzg'unchilarni axborot texnologiyalari sohasi mutaxassisi sifatiga ko'ra ajratish:

tajribasiz foydalanuvchi (A sinfi): ushbu sinfga tajovuzkor kamdan-kam uchraydigan, ammo tizimning ishlamay qolishi yoki hatto ishdan chiqishiga olib kelishi mumkin bo'lgan himoya obyektida beparvolik yoki noto'g'ri harakatlar manbai sifatida xavf tug'diradi;

ishonchli foydalanuvchi (B sinfi): buzg'unchilarning ushbu himoya obyekti buzilishining manbai bo'lishi mumkin, ammo dasturlarni o'rnatishga, tashqi manbalardan, shu jumladan Internetdan foydalanishga urinish erkin foydalanishni boshqarish tizimi va axborotni himoya qilish vositalari tomonidan to'xtatiladi;

yuqori malakali foydalanuvchi (V sinfi): ushbu sinf buzg'unchilarining kirishni boshqarish va axborotni muhofaza qilishning belgilangan qoidalarini buzishga bo'lgan barcha urinishlari xavfsizlik tizimi tomonidan bloklangan xavfsizlik auditi tizimida qayd etilishi kerak.

50. Axborot xavfsizligini buzuvchilarning modellari banking har bir muhim muhofaza obyekti bilan bog'liq ravishda tuziladi va saqlanadi shuningdek, qo'riqlanadigan obyekt tahdid modeliga kiritilgan.

51. Bank uchun axborot xavfsizligini buzuvchilarning modeli quyidagi toifalarga, xususiyatlarga va ularga nisbatan cheklov choralariga ega bo'lgan buzg'unchilarni o'z ichiga oladi:

52. Ichki buzg'unchi:

1) Bank tarmoqlari va axborot tizimlarining ro'yxatdan o'tgan (vakolatli) foydalanuvchilari bo'lgan bank xodimlari. Mumkin bo'lgan harakatlar nuqtai nazaridan ular 1-sinfga, tajriba bo'yicha esa A va B sinflariga tegishli. Ushbu qoidabuzarlar tomonidan ta'sirlanadigan asosiy himoya obyektlari: bank axborot tizimlari, lokal va korporativ tarmoqlar, ish stansiyalari, dasturiy ta'minot va elektron shakldagi ma'lumotlar.

Ushbu buzg'unchining xususiyatlari: tahdidlarni amalga oshirish qobiliyatining mavjudligi, bu asosan o'z vakolatlarini kengaytirishga urinishlar va himoyalangan obyekt bilan o'zaro aloqada bo'lish uchun faqat standart dasturiy ta'minot va texnik vositalardan foydalangan holda axborot xavfsizligini ta'minlash vositalarini yengib o'tishi himoyalangan ma'lumotlarning chiqib ketishi ehtimolini

oshiradi.

Ushbu buzg'unchilarga nisbatan cheklov choralari: huquqlarni chegaralash va himoyalanadigan obyektlarga kirishni nazorat qilish, xodimlarning axborot tizimlaridagi xatti-harakatlarini hisobga olish, mumkin bo'lgan axborotlar kanallarini monitoring qilish, konfidensial ma'lumotlarni oshkor qilmaslik talablariga rioya etilishini nazorat qilish.

2) Bankning axborot tizimlari va tarmoqlaridan foydalanishga ruxsati bo'lmagan xodimlari (qorovullar, binolarga xizmat ko'rsatuvchi texnik xodimlar va boshqalar). Mumkin bo'lgan harakatlarga ko'ra, ular 1-sinfga va tajribasi bo'yicha - A sinfiga tegishli bo'lishi mumkin. Ushbu qoidabuzarlar tomonidan ta'sirlanadigan asosiy himoya obyektlari bankning har qanday moddiy aktivlari, shu jumladan qog'ozdagi ma'lumotlardir.

Ushbu turdagi ichki buzg'unchining tahdidlarini amalga oshirish imkoniyatlari himoya qilinadigan obyektga ruxsatsiz jismoniy kirishni olishgacha kamayadi va asosan himoyalanadigan obyektga e'tibor bermaslik yoki noto'g'ri harakatlar manbai bo'lib xizmat qiladi, bu esa tizimning qisman yoki to'liq ishlamay qolishiga olib kelishi mumkin.

Ushbu buzg'unchilarga nisbatan cheklov choralari: qo'riqlash obyektlarini joylashtirish talablariga rioya qilish, ruxsatsiz jismoniy kirish va harakatlarning oldini olishga qaratilgan obyektga qarshi rejim va tashkiliy-texnik choralar kompleksidan foydalanish, muhofaza qilish obyektlari joylashgan binolarga xodimlarning kirishini boshqarish.

3) Bankning texnik vositalariga xizmat ko'rsatuvchi xodimlar. Mumkin bo'lgan harakatlar nuqtai nazaridan ular 3-sinfga va tajriba jihatidan B sinfiga tegishli. Ushbu qoidabuzarlar tomonidan ta'sirlanadigan asosiy himoya obyektlari quyidagilardir: ular xizmat ko'rsatadigan texnik vositalar (axborotni qayta ishlash va saqlash vositalari, tarmoq uskunalari va xavfsizlik vositalari ma'lumotlari), shu jumladan ularga o'rnatilgan dasturiy ta'minot va ularda saqlanadigan ma'lumotlardir.

Ushbu buzg'unchining xususiyatlari: himoyalangan obyektning apparat va dasturiy ta'minotiga kirish huquqi mavjud, ammo ularning ro'yxatdan o'tgan foydalanuvchisi emas. Ushbu turdagi buzg'unchining imkoniyatlari asosan shaxslarni himoya obyekti joylashgan binoga kirishi va ish tartibi ustidan nazoratni joriy etuvchi omillarga bog'liq.

4) Bank lokal va korporativ tarmoqlari, axborot tizimlari va axborot xavfsizligi vositalariga xizmat ko'rsatuvchi administratorlar. Mumkin bo'lgan harakatlarga ko'ra, ular 4-sinfga va tajriba bo'yicha - B va C sinflariga tegishli. Ushbu qoidabuzarlar tomonidan ta'sirlanadigan asosiy himoya obyektlari quyidagilardir: bank axborot tizimlari, ularning texnik vositalari, dasturiy ta'minotlari va ular tomonidan saqlanadigan va qayta ishlanadigan axborot tizimi ma'lumotlardir.

Ushbu buzg'unchining xususiyatlari: himoyalangan obyektga avtorizatsiya qilingan kirish imkoniyati va imtiyozli foydalanuvchilar guruhining a'zolari. Ushbu turdagi buzg'unchining o'ziga xos xususiyati shundaki, ular qo'riqlanadigan obyektning ishonchli xodimlari qatoriga kiradi va ularga qo'riqlanadigan obyekt tarkibiy qismlarining ichki holatiga ta'sir o'tkazish orqali tahdidni amalga oshirish uchun keng imkoniyatlar berilgan.

Ushbu buzg'unchilarga nisbatan cheklov choralari: himoyalanadigan obyektga kirishda ushbu xodimlarning harakatlarini hisobga olish va nazorat qilish.

5) Bank axborot tizimlarini ishlab chiquvchi mutaxassislar. Mumkin bo'lgan harakatlarga ko'ra, ular 2-sinfga, tajribaga ko'ra - A, B va V sinflariga tegishli. Ushbu qoidabuzarlar tomonidan ta'sirlanadigan asosiy himoya obyektlari quyidagilardir: axborot tizimlarining dasturiy ta'minoti va bankning axborot tizimlari.

Ushbu buzg'unchining xususiyatlari: axborot tizimi uchun dastur ishlab chiqishda yoki dastur ma'lumotlarning normal ishlashini buzish bilan bog'liq keyingi noqonuniy harakatlar uchun e'lon qilinmagan funksiyalarni (zakladkalarni) o'rnatishda ishlab chiquvchilarning xatolaridan kelib chiqadigan tahdidlarni amalga oshirish imkoniyati mavjud.

Ushbu qoidabuzarlarga nisbatan cheklov choralari: ishlab chiqish jarayonida ushbu xodimlarning harakatlarini hisobga olish va nazorat qilish, bankning alohida xodimlari tomonidan ishlab chiqilgan dasturlarni dastlabki kod analizatorlari yordamida tahlil qilish, uchinchi shaxslar tomonidan dasturning funksionalligini, kiritish va chiqish ma'lumotlarini sinovdan o'tkazish. Bank xodimlari, dasturiy ta'minot axborot xavfsizligi mahsulotlarini sertifikatlash.

53. Tashqi buzg'unchilar:

1) Bankning ishdan bo'shatilgan xodimlari. Mumkin bo'lgan harakatlar va tajriba nuqtai nazaridan ular tashkilotda ishlagan vaqtida ilgari egallagan lavozimiga qarab sinfga tegishli (tarmoqlarning va axborot tizimlarining sobiq foydalanuvchisi, texnik yordam xodimlari yoki administratorlar). Ushbu qoidabuzarlar tomonidan ta'sir ko'rsatadigan asosiy himoya obyektlari quyidagilardir: ular tomonidan Bankdagi faoliyati davomida olingan bilimlar va konfidensial ma'lumotlar.

Ushbu buzg'unchining xususiyatlari: tashqi buzg'unchi bankning himoyalangan ma'lumotlarini oshkor qilishi, shu jumladan ruxsatsiz kirish va axborot xavfsizligi vositalarini chetlab o'tishi, noqonuniy xatti-harakatlarni sodir etishi sobiq tashkilotga zarar yetkazish uchun texnologik va texnik ma'lumotlarni oshkor qilishi kabi tahdidlarni amalga oshirish imkoniyatlari mavjud.

Ushbu buzg'unchilarga nisbatan cheklov choralari: ishdan bo'shatilgan xodim konfidensial ma'lumotlarni oshkor qilmaslik bo'yicha majburiyatlarni bajarishi, ishdan bo'shatilgandan keyin ularning qayd yozuvlaridan foydalanish imkoniyatini istisno qilish.

2) Bankda o'z faoliyatini amalga oshirish imkoniyatiga ega bo'lgan, uchinchi tomon tashkilotlari vakillari bo'lgan tashrif buyuruvchilar. Ushbu qoidabuzarlar ta'sir qiladigan asosiy himoya obyektlari quyidagilardir: mijoz foydalanishi uchun taqdim etilgan aktivlar, shuningdek ularga kirish huquqi berilgan axborot tizimlari.

Ushbu buzg'unchining xususiyatlari: ushbu turdagi tashqi buzg'unchining tahdidlarini amalga oshirish imkoniyatlari himoya obyektiga ruxsatsiz jismoniy kirishga qadar bo'ladi.

Ushbu buzg'unchilarga nisbatan cheklov choralari: qo'riqlash obyektlarini joylashtirish bo'yicha talablarni bajarish, xavfsizlik va tashkiliy-texnik chora-tadbirlar majmuidan foydalangan holda mehmonlarning ular uchun ruxsat etilmagan binolarga (zonalarga) kirishini cheklash.

3) Bankda biror bir vazifani (xizmat ko'rsatuvchi provayderlarni) amalga

oshiradigan uchinchi tomon tashkilotlari vakillari bo'lgan tashrif buyuruvchilar. Mumkin bo'lgan harakatlar nuqtai nazaridan ular 2-4 sinflarga va tajriba nuqtai nazaridan - B va V sinflariga tegishli bo'lishi mumkin. Ushbu qoidabuzarlar tomonidan ta'sirlanadigan asosiy himoya obyektlari quyidagilardir: kirish huquqi berilgan va ular tomonidan xizmat ko'rsatadigan apparat va dasturiy ta'minot.

Ushbu buzg'unchining xususiyatlari: himoyalangan obyektga avtorizatsiya qilingan kirish imkoniyati mavjudligi, lekin ularning ro'yxatdan o'tgan foydalanuvchi bo'lmagan - himoyalangan obyektning apparat va dasturiy ta'minotini ishlab chiquvchilar, ularni o'rnatish, ishga tushirish, xizmat ko'rsatishni amalga oshiruvchilar va boshqalar. Ushbu turdagi buzg'unchining o'ziga xos xususiyati shundaki, u maxsus buzg'unchi vositalarga kiritilgan ishlash algoritmiga qarab turli harakatlarni amalga oshirishi mumkin.

Ushbu qoidabuzarlarga nisbatan cheklov choralari: ish tartibini nazorat qilish, ushbu ishlarni bajarishda bank vakilining ishtirok etishi, faqat muhofaza qilinadigan obyektning zarur vositalariga kirishni ta'minlash, ushbu kirishni nazorat qilish, mahsulotni loyihalashda texnik talablarga rioya qilish; "oq xakerlar" tamoyili bo'yicha zaifliklarni sinovdan o'tkazish.

4) Himoya tizimini chetlab o'tib, tashqi tarmoq orqali muhofaza qilinadigan obyektga ruxsatsiz kirish huquqini olgan buzg'unchilar. Malakasiga ko'ra, bu buzg'unchi V sinfiga tegishli va mumkin bo'lgan harakatlarga ko'ra u 2 va 3 sinflarga tegishli bo'lishi mumkin. Ushbu qoidabuzarlar ta'sir ko'rsatadigan asosiy himoya obyektlari quyidagilardir: Bankning lokal va korporativ tarmoqlari va ularga ulangan axborot resurslari va axborot tizimlari.

Ushbu tajovuzkorning xususiyatlari: tizimdagi maxsus dasturiy ta'minot yoki apparat vositalaridan yoki zaifliklardan foydalangan holda maqsadli harakatlarni amalga oshirish.

Ushbu buzg'unchilarga nisbatan cheklov choralari: ushbu buzg'unchilarning ruxsatsiz harakatlarining oldini olishga qaratilgan apparat va dasturiy ta'minotni muhofaza qilish choralari kompleksidan foydalanish.

VIII. Axborot xavfsizligi choralari

54. Bankda MBBTni qurish uchun axborot xavfsizligining barcha choralari ko'riladi va ular quyidagilardan iborat:

huquqiy choralar;

xulqiy va axloqiy(psixologik) choralar;

tashkiliy choralar;

texnologik choralar;

muhandislik-texnik choralar;

dasturiy va texnik choralar;

tashqi foydalanuvchilar bilan munosabatlarda xavfsizlik choralari.

Huquqiy choralar (hujjatlar bilan ta'minlash choralari)

55. Bankda normativ-huquqiy qo'llab-quvvatlash chora-tadbirlari Bank axborot xavfsizligini boshqarishda rahbarlik qiladigan me'yoriy hujjatlar bazasini shakllantirishga qaratilgan.

56. Bankning axborot xavfsizligini ta'minlash sohasidagi me'yoriy-huquqiy

bazasi O‘zbekiston Respublikasi davlat standartlarini o‘z ichiga olgan huquqiy va me’yoriy hujjatlarni, shuningdek, Bankning axborot xavfsizligini ta’minlash masalalarini tartibga soluvchi ichki hujjatlarini o‘z ichiga oladi.

57. Bankning axborot xavfsizligini ta’minlash sohasidagi normativ-huquqiy bazasi Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan shakllantiriladi va yuritiladi.

58. Bankning axborot xavfsizligi bo‘yicha me’yoriy-huquqiy bazasi elektron va qog‘oz ko‘rinishda yuritiladi.

59. Bankning axborot xavfsizligini ta’minlash sohasidagi ichki hujjatlari Xavfsizlik va axborotlarni muhofaza qilish departamenti va uning tarkibiy bo‘linmalari, shuningdek, Axborot texnologiyalari departamenti tomonidan ishlab chiqiladi.

Shuningdek, mazkur bo‘linmalar bankning axborot xavfsizligini ta’minlash sohasidagi normativ-huquqiy bazasini takomillashtirish bo‘yicha takliflar kiritadi va chora-tadbirlar ishlab chiqadi.

60. Bankning axborot xavfsizligi sohasidagi ichki hujjatlari quyidagi darajadagi hujjatlardan iborat:

a) asosiy hujjat - bankning axborot xavfsizligi siyosati;

b) himoya qilish obyektlarini belgilaydigan va tasniflovchi hujjatlar (ro'yxatlar va tasniflagichlar);

c) Vazifalar va majburiyatlarni taqsimlovchi hujjatlar (tarkibiy bo'linmalar nizomi, lavozim yo’riqnomalari);

d) axborot xavfsizligini boshqarish jarayonlari va tartiblarini tartibga soluvchi hujjatlar (nizomlar, tartiblar, qoidalar, reglamentlar, yo’riqnomalar, usullar);

e) axborot xavfsizligi chora-tadbirlarini amalga oshirishga qaratilgan tashkiliy-ma'muriy hujjatlar (buyruqlar, farmonlar, rejalar);

f) obyektlar va himoya vositalariga talablarni belgilovchi hujjatlar (talablar, texnik topshiriqlar, loyihalar);

g) ishga tushirish va foydalanish hujjatlari (qo'llanmalar, foydalanish yo'riqnomalari);

h) Axborot xavfsizligini ta'minlash bo'yicha bajarilgan protseduralar va ishlarni ro'yxatdan o'tkazish va tasdiqlash uchun foydalaniladigan hujjatlar (ish shakllari, jurnallar, hisobotlar, arizalar, protokollar, aktlar).

61. Axborot xavfsizligi bo‘yicha ichki hujjatlar va ularda belgilangan talablar Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan bank tegishli xodimlariga yetkaziladi va ushbu xodimlar tomonidan qat’iy rioya qilinishi shart.

62. Axborot xavfsizligi bo'yicha ichki me'yoriy hujjatlarning alohida turlari siyosatning ilovalarida keltirilgan.

Xulqiy va axloqiy (psixologik) axborot himoyasi choralar

63. Axborotni himoya qilishning xulqiy va axloqiy (psixologik) choralari quyidagilarga qaratilgan bo’lishi kerak:

xodimlar jamoasida sog’lom axloqiy muhitni yaratish;

inson omili bilan bog’liq bo’lgan salbiy xatti-harakatlar va axborot xavfsizligini buzish ehtimolini kamaytirish;

axborotni muhofaza qilish rejimi buzilgan taqdirda shaxsiy psixologik omillarni chiqarib tashlash;

bank xodimlari tomonidan etika qoidalariga amal qilinishi.

64. Xulqiy va axloqiy himoya choralari profilaktik bo'lib, quyidagilarni o'z ichiga oladi:

bank xodimlar o'rtasida tushuntirish ishlarini olib borish;

psixologik monitoring;

huquqbuzarlarga nisbatan majburlash va intizomiy jazo choralarini qo'llash;

xodimlarni rag'batlantirish.

65. Tushuntirish ishlari Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan maxsus darslar yoki individual suhbatlar shaklida olib boriladi. Ushbu tushuntirish ishlarini amalga oshirish uchun bank Xodimlarni boshqarish departamenti xodimlari jalb etiladi.

66. Ushbu tushuntirish ishlari quyidagi maqsadda olib boriladi:

xodimlar bank faoliyatiga tahdidlarning ta'siri va yuzaga kelishi mumkin bo'lgan oqibatlar, shuningdek buzg'unchilarga nisbatan qo'llanilishi mumkin bo'lgan javobgarlik choralari to'g'risidagi tushuntirish ishlarini olib borish;

xodimlar o'rtasida siyosatining elementlari va talablarini bajarish zarurati to'g'risida xabardorlikni oshirish;

xodimlarning axborot xavfsizligini ta'minlash masalalarida bilish darajasi va javobgarlik hissini oshirish;

bank xodimlari o'rtasida axborot xavfsizligini ta'minlash qoidalari va talablariga rioya etilishiga ko'maklashuvchi talab qilinadigan xulq-atvor va axloq normalarini ishlab chiqish;

axborot xavfsizligini ta'minlash muammolarini hal qilishda xodimlarning hamjihatligini oshirish.

Bu tushuntirish ishlari xodimlarga nisbatan ishda, ham ishga joylashishda olib boriladi.

67. Tushuntirish ishlari bank xodimlarining quyidagi guruhlari uchun yiliga kamida bir marta alohida amalga oshiriladi:

bankning bank mijozlari bilan bevosita muloqotda bo'lmagan xodimlari;

bank xodimlarining bank mijozlari bilan o'zaro aloqalari;

bankning axborot tizimlari va resurslariga, bank axborot infratuzilmasini texnik va texnologik jihozlariga xizmat ko'rsatishni ta'minlovchi bank xodimlari.

bank texnik xodimlari.

68. Bankning yangi xodimlariga nisbatan axborot xavfsizligini ta'minlash masalalari bo'yicha instruktaj o'tkaziladi.

69. Psixologik monitoring jismoniy shaxsga ham, tuzilmaviy bo'linmalarga ham, umuman olganda Bankka nisbatan ham qo'llaniladi, bu xodimlar o'rtasida yuzaga kelgan har qanday tartibsizliklarni tezkorlik bilan aniqlash, me'yor va qoidalarga rioya qilish bo'yicha mas'uliyatli va vijdonli xodimlarni, mas'uliyatsizlik va e'tiborsizlikni aniqlash imkonini beradi. nazorat qilinishi kerak bo'lgan xodimlar va/yoki ularga nisbatan tegishli choralar ko'rilishi kerak.

70. Kerakli choralari bank xodimlarini axborot xavfsizligini ta'minlash bo'yicha qoidalar va talablarga, xususan, ular buzilgan taqdirda jazo choralariga rioya qilishga kerak bo'lgani uchun sharoit yaratishga qaratilgan bo'lishi kerak.

71. Qoidabuzarlarga nisbatan bank rahbariyati tomonidan mehnat shartnomalari va kontraktlar doirasida mehnat qonunchiligiga muvofiq tanbeh yoki jarima tarzidagi intizomiy jazo choralari qo‘llanilishi mumkin.

72. Rag‘batlantirish choralari bank xodimlarini to‘g‘ri xulq-atvorga undaydigan shart-sharoitlarni yaratishga qaratilgan bo‘lishi kerak. Ushbu chora-tadbirlar rag'batlantirish choralarini o'z ichiga oladi.

73. Mehnat majburiyatlarini munosib bajarayotgan intizomli xodimlarga nisbatan rag’batlantirish choralari minnatdorchilik e’lon qilish, faxriy yorliqlar, pul mukofoti yoki qimmatbaho sovg’a bilan ta’minlash shaklida amalga oshirilishi kerak va maxsus xizmatlari uchun ular qonun hujjatlarida belgilangan tartibda davlat mukofotlari bilan taqdirlanishi mumkin.

74. Bank xodimlari huquqbuzarliklarning oldini olish, ularni sodir etishiga sabab bo‘lgan shart-sharoitlarni bartaraf etish maqsadida bank rahbariyati tomonidan belgilanadigan bank xodimlarining odob-axloq qoidalariga rioya etishlari shart.

Tashkiliy choralar

75. Bankda tashkiliy tadbirlar quyidagilarga qaratilgan:

xodimlarning xavfsizligi, xabardorligi va o'qitilishi;

himoyalangan obyektlarga jismoniy kirishni cheklash (jismoniy xavfsizlik);

konfidensial ma'lumotlarni himoya qilish;

axborotni himoya qilish tizimi va vositalarini yaratish, faoliyat yuritish va rivojlantirish;

axborot xavfsizligi hodisalariga javob berish;

xavfsizlik holatini nazorat qilish va baholash.

76. Bankda axborot aktivlarini aniqlash va ularni himoya qilish bo‘yicha tegishli javobgarlikni belgilash maqsadida axborot aktivlarini boshqarish bo‘yicha tashkiliy chora-tadbirlar amalga oshiriladi.

Bank axborot aktivlarini boshqarish bo‘yicha tashkiliy chora-tadbirlar quyidagilardan iborat:

a) axborot resurslari va tegishli axborotni qayta ishlash vositalarini aniqlash uchun axborot aktivlarini inventarizatsiya qilish;

b) axborot aktivlarini hisobga olish - ushbu aktivlarning inventar ro'yxatini tuzish va uni yangilab turish;

c) axborot aktivlariga egalik qilish - axborot aktivlari egalarini tayinlash, ularning axborot aktivlariga nisbatan majburiyat va javobgarliklarini belgilash;

d) axborot aktivlarini tasniflash – bank uchun ahamiyati, muhimligi va sezgirligi qonun hujjatlari talablariga muvofiq axborot aktivlarini tasniflash, shuningdek ularni himoya qilishning tegishli darajasini ta’minlash;

e) axborot aktivlarini markalash – bank tomonidan qabul qilingan tasniflash tizimiga muvofiq axborot aktivlarini markalash tartib-qoidalari majmuasini ishlab chiqish va amalga oshirish;

f) axborot aktivlaridan maqbul foydalanish va boshqarish - axborot aktivlari va tegishli axborotni qayta ishlash vositalaridan maqbul foydalanish va boshqarish qoidalarini hujjatlashtirish va amalga oshirish.

Bankda axborot aktivlarini inventarizatsiya qilish, hisobga olish, egalik qilish, tasniflash, yorliqlash, reyestrni shakllantirish, shuningdek ularni

boshqarishning boshqa tartiblari siyosatning 13-ilovasida keltirilgan Axborot aktivlarini boshqarish tartibiga muvofiq amalga oshiriladi.

Himoya qilish obyektlari va axborot aktivlarini aniqlash bo‘yicha inventarizatsiya Xavfsizlik va axborotlarni muhofaza qilish departamenti va Axborot texnologiyalari departamenti bilan birgalikda yiliga kamida bir marta tashkil etiladi va o‘tkaziladi. Inventarizatsiya natijalariga ko‘ra, zarur hollarda qo‘riqlanadigan obyektlar ro‘yxatiga, axborot aktivlari (resurslari) reyestriga va bankning konfidensial ma’lumotlar ro‘yxatiga o‘zgartirish va qo‘shimchalar kiritiladi. Bundan tashqari, inventarizatsiya natijalariga ko'ra binolarning ro'yxati, ularga kiritilgan apparat va dasturiy ta'minot majmuasining tarkibi aniqlanadi.

Himoya qilinadigan obyektlarni kategoriyalash va tasniflash O‘zDSt 2814:2014 “Axborot texnologiyalari. Avtomatlashtirilgan tizimlar. Axborotga ruxsatsiz kirishdan himoyalanish darajasi bo‘yicha tasnifi” va boshqa me’yoriy hujjatlar talablari. Himoya qilinadigan obyektlarni tasniflash Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan amalga oshiriladi.

77. Bankda xodimlarning xavfsizligini ta’minlash, ularni xabardor qilish va o‘qitish bo‘yicha tashkiliy chora-tadbirlar quyidagilarni o‘z ichiga oladi:

a) ishga qabul qilishda:

axborot xavfsizligini ta'minlash uchun mas'ul bo'lgan mutaxassislarga va ishi axborotni qayta ishlash va axborot xavfsizligini ta'minlash jarayonlari bilan bog'liq bo'lgan xodimlarning malakasi darajasiga qo'yiladigan malaka talablarini belgilash.;

ishga qabul qilinuvchilarni bilim va kompetensiya darajasining bank tomonidan ishga qabul qilishda belgilangan malaka va qobiliyat talablariga muvofiqligini tekshirish;

b) ishga joylashishda:

mehnat shartnomalarida axborot xavfsizligi sohasida javobgarlikni belgilash;

ushbu siyosat bilan tanishish;

axborot Xavfsizligini ta’minlash sohasidagi lavozim yo‘riqnomalarida belgilangan vakolatlar, majburiyat va javobgarlik, shuningdek Bankda axborot xavfsizligi talablariga rioya qilmaganlik uchun rag‘batlantirish va intizomiy javobgarlikka tortish bo‘yicha ko‘rilayotgan chora-tadbirlardan xabardor bo‘lish;

maslahatlar va / yoki instruktaj, axborot xavfsizligi bo'yicha tavsiyalar olish;

c) ish paytida:

xabardorlikni oshirish, ta'lim va trening;

axborot xavfsizligini ta'minlash uchun mas'ul bo'lgan xodimlarni qayta tayyorlash va malakasini oshirish (zaruri kompetensiyalarni olish);

bank xodimlarining xabardorlik darajasi va malakasini tekshirish yoki baholash;

xodimlarni ushbu siyosat qoidalari va talablari, axborot xavfsizligi sohasidagi me'yoriy hujjatlar to'g'risida xabardor qilish;

xodimlar tomonidan protseduralar va axborot xavfsizligi talablari bajarilishini nazorat qilish;

intizomiy jazo choralarini belgilash va ko’rish.

d) ishdan bo'shatilganda yoki ish joyi o'zgartirilganda:

ishni tark etgan yoki o'zgartirgan xodim bilan mehnat shartnomasi bekor qilinganidan keyin 5 yil ichida oshkor etilmaslik kerak bo'lgan konfidensial majburiyatini belgilash;

ishdan bo'shagan yoki ish joyini o'zgartirganlarga konfidensial ma'lumotlar, ular mehnat davrida foydalangan ma'lumotlarni qayta ishlash, uzatish va saqlash vositalarini qaytarib olish;

ishdan ketgan yoki ish joyini o‘zgartirgan xodimlarning bank himoya obyektlariga mantiqiy va jismoniy kirishning barcha huquqlaridan bekor qilish.

Axborot xavfsizligini ta'minlash uchun mas'ul bo'lgan mutaxassislarga qo'yiladigan malaka talablari, ishi axborotni qayta ishlash jarayonlari bilan bog'liq bo'lgan xodimlarning malaka darajasi, shuningdek ularning vazifalari Xavfsizlik va axborotlarni muhofaza qilish departamenti, shuningdek Axborot texnologiyalari departamenti tomonidan belgilanadi.

Mehnat shartnomalarida axborot xavfsizligini ta’minlash sohasidagi javobgarlik va majburiyatlarni belgilash, shuningdek, ular haqida bank xodimlarini boshqarish departamenti vakolatiga kiradi.

Bankda xabardorlik malakasini oshirish, o’qitish va kadrlar tayyorlash, shuningdek, axborot xavfsizligi sohasidagi xabardorlik va malaka darajasini baholash bo‘yicha chora-tadbirlar muntazam ravishda amalga oshirish.

Axborot xavfsizligini ta’minlashga mas’ul bo‘lgan xodimlarning malakasini oshirish, shuningdek bank xodimlarini axborot xavfsizligi bo‘yicha o‘qitish maqsadida Xavfsizlik va axborotlarni muhofaza qilish departamenti har yili o’qitish va mutaxassislarning malaka oshirish treninglar kurslari jadvalini tuzadi va tasdiqlaydi. Mutaxassislar malakasini oshirish ta’lim muassasalarida axborot xavfsizligini ta’minlash bo‘yicha, bank xodimlarini o‘qitish esa Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan tashkil etilib olib boriladi.

Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan bank xodimlarining axborot xavfsizligi sohasidagi bilimlarini oshirish, o‘z majburiyatlari va javobgarliklarini anglash maqsadida o‘quv seminarlar o‘tkaziladi.

bank xodimlari va mutaxassislarining xabardorlik darajasini tekshirish yoki baholash Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan bank xodimlarini va uning alohida mutaxassislarini, seminarlar o‘quv mashg‘ulotlari natijalari bo‘yicha attestatsiyadan o‘tkazish, testdan o‘tkazish va so‘roq qilish yo‘li bilan amalga oshiriladi.

Bank quyidagi maqsadlarda bank xodimlariga nisbatan intizomiy jazo choralarini qo‘llaydi:

bankning axborot xavfsizligi siyosati yoki tartib-qoidalarini buzgan bank xodimlarining intizomiy javobgarligini belgilash;

bank xodimlarini ushbu siyosat yoki axborot xavfsizligi tartib-qoidalarining buzilishi hamda axborot xavfsizligini ta’minlashning boshqa har qanday buzilishining oldini olish;

axborot xavfsizligini qasddan buzganlik uchun javobgar shaxslarni javobgarlikka tortish;

xodimlarni axborot xavfsizligi masalalariga mas'uliyat bilan munosabatda bo'lishga motivatsiya va rag'batlantirish.

78. Himoya qilinadigan obyektlarga jismoniy kirishni cheklash bo'yicha

tashkiliy chora-tadbirlar (jismoniy xavfsizlik) bank qo'riqlanadigan obyektlarga ruxsatsiz jismoniy kirish, shikastlanish va boshqa salbiy ta'sirlarning oldini olishga qaratilgan.

Bank hududi, bank binolari va uning tarkibiy bo‘linmalari bank xonalarining jismoniy xavfsizligi perimetrlarini aniq belgilab qo‘yishi kerak.

Bank binosi va xonalari jismoniy himoya qilish perimetrlari quyidagi xavfsizlik zonalariga bo'linadi:

1) past xavfsizlik zonalari (1-xizmat maydoni - front zona) - ruxsat etilmagan shaxslarning mavjudligiga ruxsat berilgan xona va joylar - (axborot xonasi, amaliyot xonasi, kredit xonasi va boshqalar) mijozlar, tashrif buyuruvchilar va boshqalar, oldindan ruxsatisiz va shaxsni tasdiqlovchi hujjatlarni taqdim etmasdan kirish.

2) o'rtacha xavfsizlik zonalari (2-xizmat zonasi) - faqat bank xodimlariga ruxsat beriladigan xonalar va joylar (amaliyot bo’linmasi, tarkibiy bo'linmalarning xizmat xonalari va unga tutash yo'laklar), shuningdek bir martalik, vaqtinchalik yoki doimiy ruxsatnomalari bo'lgan tashrif buyuruvchilar;

3) muhim himoyalangan zonalar (3-himoyalangan zona) - bank xodimlarining ma'lum bir muhim doirasiga kirishiga ruxsat berilgan va muhim resurslar joylashtirilgan himoya qilinadigan xonalar yoki joylar (kassa xonalari, moddiy boyliklarni saqlash) aktivlar - omborlar, pul omborlari, server xonalari ma'lumotlarni qayta tiklash markazi xonalari va boshqalar).

Hududlarni himoya qilish darajasidan kelib chiqib, ularga Bankning tegishli aktivlari joylashtirilishi kerak. Muhim himoya obyektlari yuqori xavfsizlik zonalarida joylashgan. Yuqori darajadagi xavfsizlik zonalari bankning jismoniy xavfsizlik perimetridan imkon qadar uzoqroqda joylashgan bo'lishi va past darajadagi xavfsizlik zonalariga yonma-yon bo'lmasligi kerak.

Bankda jismoniy xavfsizlikni ta’minlashning tashkiliy chora-tadbirlariga quyidagilar kiradi:

a) qo'shni hududlar, binolar va xonalarga nisbatan:

bank bosh ofisi (AB) va uning MBXO va BXM hududi va binolariga kirishda qo‘riqlashni tashkil etish;

bank hududi va binolariga bank xodimlari va tashrif buyuruvchilarga doimiy qo'shni hududga kirish va chiqish, vaqtinchalik yoki bir martalik yo‘llanma, moddiy boyliklar va mol-mulkni olib kirish hamda olib chiqish uchun moddiy ruxsatnomalar, avtotransport vositalariga ruxsatnomalar berish orqali kirish nazoratini ta’minlash;

bank tashrif buyuruvchilarni hisobga olishning markazlashtirilgan yagona ma’lumotlar bazasini joriy etish;

bank bosh ofisi va ab, tkxm va kxm binolarini qo‘riqlash zonalariga bo‘lish;

bank mijozlari va tashrif buyuruvchilarni faqat amaliyot va qabul xonalarida qabul qilish va ularga xizmat ko‘rsatish (1-zona);

axborotlashtirish obyektlarini nazorat qilinadigan zona chegarasiga nisbatan maksimal mumkin bo'lgan masofada va ularning axborotni qayta ishlash, axborotni uzatish va himoya qilishning texnik vositalarini - ma'lumotlarni qayta ishlash markazining himoyalangan server xonalarida (3 zonali) joylashtirish;

binolarda (2 zonali) va/yoki xizmat ko'rsatish xonalarida tashrif buyuruvchilarni kuzatib borish;

3-zonaning qo'riqlanadigan binolariga qabul qilingan shaxslar ro'yxatini aniqlash;

xizmat binolarining kalitlarini saqlash va ularni ish soatlaridan keyin himoya qilish uchun kampuslardan foydalanish, shuningdek yozuvlarni yuritish va ularni xodimlarga imzo qo'ymasdan berish;

b) axborotni qayta ishlash, saqlash, uzatish va himoya qilish vositalari haqida:

himoyalangan xonalarda vositalarni joylashtirish;

qulflanadigan kommutatsiya shkaflarida vositalarni o'rnatish;

uskunaning tashqi korpusida qulflar, bir martalik muhrlar, himoya yopishqoq lentalar yoki himoya va gologrаfik yorliqlardan foydalanish;

c) qog'oz ko'rinishidagi konfidensial ma'lumotlarga, konfidensial ma'lumotlarni o'z ichiga olgan tashuvchilarga va texnologik jarayonlarda foydalaniladigan tashuvchilarga nisbatan:

seyflar, qulflanadigan temir shkaflar va boshqa xavfsiz saqlash vositalaridan foydalanish;

jurnallarda qayd etish.

d) elektr ta'minoti kabellari va tarmoq kabellariga nisbatan siyosatning 13-bo'limida ko'rsatilgan ma'lumotlarning ushlanishi va ularning shikastlanishining oldini olish uchun ularni ochilishdan himoya qilish bo'yicha tashkiliy choralar ko'riladi.

Bank obyektlari qo‘riqlanishini tashkil etish O‘zbekiston Respublikasi Ichki ishlar vazirligi va Markaziy bank Boshqaruvining 2010-yil 5-iyundagi 12-son, qarori talablari asosida amalga oshiriladi. “O‘zbekiston Respublikasi Ichki ishlar organlari qo‘riqlash bo‘linmalari tomonidan Banklar va ularning filiallari xavfsizligini ta’minlashni tashkil etish bo‘yicha yo‘riqnomani tasdiqlash to‘g‘risida”gi 22/7- XDFU qarori bilan belgilangan.

Bank barcha obyektlarini qo‘riqlash shartnoma asosida Milliy gvardiya tomonidan amalga oshiriladi.

79. Konfidensial ma'lumotlarni himoya qilish bo'yicha tashkiliy choralarga quyidagilar kiradi:

a) Bankning konfidensial ma’lumotlarni tashkil etuvchi ma’lumotlar ro‘yxatini belgilash, shuningdek zarur hollarda ushbu ro‘yxatga o‘zgartirish va qo‘shimchalar kiritish;

b) Bankning konfidensial ma’lumotlarga ruxsat berilgan qo‘yilgan xodimlari ro‘yxatini aniqlash;

c) Bank xodimlari tomonidan bank konfidensial ma’lumotlarini oshkor etmaslik bo‘yicha majburiyatlarni qabul qilish;

d) Bank kontragentlari bilan tuziladigan shartnomalarda (konfidensial shartnomasi) konfidensial ma’lumotlarni oshkor qilish shartlari, talablari majburiyatlari va javobgarligini belgilash;

e) Konfidensial ma'lumotlar va ularning moddiy tashuvchilari uchun konfidensial belgilaridan foydalanish;

f) Konfidensial ma'lumotlarga ega qog'oz va elektron tashuvchilarda konfidensial ma'lumotlarni ro'yxatga olish va hisobga olish;

g) Konfidensial ma'lumotlarni lokal, korporativ va tashqi tarmoqlar, elektron pochta, elektron hujjat aylanish tizimi orqali uzatish uchun cheklovlar yoki himoya talablarini belgilash, shuningdek, konfidensial ma'lumotlarni Internet-resurslarda, ijtimoiy tarmoqlarda, ommaviy axborot vositalarida va boshqalarda tarqatish bo'yicha cheklovlarni belgilash;

h) axborotni qayta ishlash vositalari, elektron tashuvchilar, mobil qurilmalar va boshqalarda qog'oz va elektron shaklda konfidensial ma'lumotlarni saqlash uchun cheklovlar yoki himoya talablarini belgilash;

i) konfidensial ma'lumotlarga kirish va ulardan foydalanish tartiblarini belgilash;

j) konfidensial ma'lumotlar qayta ishlanadigan va saqlanadigan binolar ro'yxatini aniqlash, shuningdek ularga ruxsatsiz jismoniy kirishdan himoyalanish talablarini belgilash;

k) konfidensial ma'lumotlarga ega elektron tashuvchilarni saqlash, hisobdan chiqarish va yo'q qilishga qo'yiladigan talablarni belgilash;

l) elektron shaklda konfidensial ma'lumotlarni qayta ishlash va saqlash uchun foydalaniladigan axborotlashtirish obyektlarini aniqlash, shuningdek ularga ruxsatsiz mantiqiy kirishdan himoya qilish uchun talablarni belgilash;

m) Bank xodimlari tomonidan ishdan bo'shatilgan yoki o'zgartirilgan taqdirda, konfidensial ma'lumotlarni moddiy tashuvchiga qaytarish bo'yicha talablarni belgilash;

n) konfidensial axborotni himoya qilish bo'yicha talablarga rioya etilishi ustidan nazoratni ta'minlash.

Himoya qilinishi kerak bo'lgan axborot bilan ishlash tartibi O‘zbekiston Respublikasining davlat sirlarini himoya qilish masalalari bo‘yicha idoralararo komissiyaning Raisi Bosh vazir o'rinbosari tomonidan 2006 yil 5 dekabrda tasdiqlangan, tarqatilishi cheklangan, konfidensial bo'lmagan ma'lumotlarni o'z ichiga olgan hujjatlar, fayllar va nashrlarni hisobga olish, muomalada bo'lish va saqlash tartibi to'g'risidagi yo'riqnomaga muvofiq amalga oshirilishi kerak.

Bankda konfidensial ma’lumotlarni himoya qilish bo‘yicha chora-tadbirlarni amalga oshirish tartibi siyosatning 16-ilovasida keltirilgan Konfidensial axborotni himoya qilish bo‘yicha yo‘riqnomada belgilangan.

80. Axborotni himoya qilish tizimi va vositalarini yaratish, faoliyat yuritishi va rivojlanishi bo'yicha quyidagi tashkiliy chora-tadbirlar amalga oshiriladi:

a) Bankning axborot xavfsizligini ta’minlash bo‘yicha chora-tadbirlarni amalga oshirish doirasida axborot xavfsizligi vositalarini xarid qilish;

b) xarid qilinadigan axborot xavfsizligi vositalariga texnik talablarni aniqlash;

c) xonalarni ajratish, foydalanish yo'riqnomalarini ishlab chiqish, mas'ul xodimni tayinlash va uni ekspluatatsiyaga o'qitishni o'z ichiga olgan tizim va axborot xavfsizligi vositalarini joriy etish va saqlashga tayyorgarlik ko'rish bo'yicha tashkiliy chora-tadbirlarni amalga oshirish;

d) axborot xavfsizligi vositalarini joriy etishda tajriba va qabul qilish sinovlarini o'tkazish;

e) himoya tizimini boshqarish (boshqaruv), shu jumladan konfiguratsiya va sozlamalarni nazorat qilish, ishlash qobiliyatini tiklash, dasturiy ta'minotni

yangilashni o'rnatish, operatsion hujjatlarni sozlash, xavfsizlik hodisalarini nazorat qilish, nazorat qilish protseduralari va natijalarini hujjatlashtirish;

f) axborot xavfsizligi tizimining ishlashi va xavfsizligini ta'minlashda kamchiliklar aniqlangan taqdirda uni takomillashtirish bo'yicha takliflar tayyorlash va kiritish.

Bankda axborotni himoya qilish tizimi va vositalarini yaratish, faoliyat ko‘rsatishi va rivojlantirish bo‘yicha ushbu bandda nazarda tutilgan tashkiliy chora-tadbirlar Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborot va kartochkalar tizimi xavfsizligi bo’limi tomonidan, shuningdek MBXOni Xavfsizlik va axborotni muhofaza qilish bo’limi, bank boshqa bo‘linmalari bilan hamkorlikda amalga oshiriladi.

81. Bank axborot xavfsizligi hodisalariga munosabat bildirish bo‘yicha siyosatning 9-bo‘limida belgilangan tashkiliy choralarni ko‘radi.

82. Bankda xavfsizlikni nazorat qilish va baholashning tashkiliy chora-tadbirlari qo‘llaniladi:

bank AXBTning zaif tomonlari va kamchiliklarini aniqlash;

tahdidlardan himoyalangan obyektlarni himoya qilish holatini obyektiv baholash;

AXBT va unda qo'llaniladigan axborotni himoya qilish usullari va vositalarining ushbu siyosat va me'yoriy hujjatlar talablariga muvofiqligini aniqlash;

qo'llaniladigan xavfsizlik choralari va vositalarining samaradorligini baholash;

tashkilotning axborot xavfsizligi maqsadlariga erishishini baholash va boshqalar.

Bankda xavfsizlik holatini nazorat qilish va baholash maqsadida quyidagi tashkiliy chora-tadbirlar ko‘riladi:

a) Xavfsizlik tahlili qoidalariga muvofiq bankning axborot xavfsizligi zaif tomonlarini izlash va tahlil qilish;

b) himoya qilish obyektlarining himoya darajasini baholash, shuningdek ushbu siyosatning dolzarbligi va samaradorligini baholash uchun ichki va tashqi auditlarni o'tkazish;

c) O‘zbekiston Respublikasi Prezidentining 2011 yil 8 iyuldagi “Milliy axborot resurslarini muhofaza qilish bo‘yicha chora-tadbirlari to‘g‘risida”gi 1572 – sonli qaroriga muvofiq akkreditatsiyadan o‘tgan tashkilotlar tomonidan bankning axborotlashtirish obyektlarini attestatsiyadan o‘tkazish;

d) Bank rasmiy web-saytini axborot xavfsizligi talablariga muvofiqligini ekspertizadan o‘tkazish;

e) Bankda mavjud axborot tizimlarini modernizatsiya qilish va yangilarini yaratish bo‘yicha texnik topshiriqlarni, shuningdek, yangi joriy etilayotgan axborot tizimlarining axborot xavfsizligi talablariga muvofiqligi bo‘yicha ekspertizasini o’tkazish;

f) Bank tomonidan mustaqil ishlab chiqilgan dasturiy ta’minotni axborot xavfsizligi talablariga muvofiqligini sertifikatlash;

g) ko‘rilgan tashkiliy, texnik va boshqa himoya choralari samaradorligini baholash shuningdek, (audit) ekspertiza va sertifikatlashtirish natijalari bo‘yicha

aniqlangan kamchiliklarni bartaraf etish;

Ichki auditning muntazamligi yiliga kamida bir marta, tashqi audit esa kamida uch yilda bir marta o‘tkazilishi lozim.

Ichki auditni axborot xavfsizligi bo‘yicha mas’ul xodim bankning Axborot texnologiyalari departamenti mutaxassislarini jalb qilgan holda amalga oshiradi. Axborot xavfsizligining tashqi auditini o‘tkazish uchun bunday auditni o‘tkazishga vakolatli uchinchi tomon tashkilotlari jalb qilinadi.

Xavfsizlikni nazorat qilish va baholashning boshqa tadbirlarini, shu jumladan attestatsiya, ekspertiza, baholash va boshqalarni o'tkazishni tashkil etish Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan amalga oshiriladi.

Audit va boshqa tekshiruvlar natijalari hujjatlashtirilishi kerak, ular ko'rsatilishi kerak:

aniqlangan zaifliklar, kamchiliklar va nomuvofiqliklar;

rioya qilmaslik sabablari;

muvofiqlikka erishish uchun harakat qilish zarurati va harakatlarning o'zi;

himoya choralari va vositalarining samaradorligini baholash va boshqalar.

Xavfsizlik va axborotlarni muhofaza qilish departamenti audit va boshqa tekshirishlar natijalariga ko‘ra aniqlangan zaifliklar, kamchiliklar va nomuvofiqliklarni bartaraf etish, himoya qilish samaradorligini oshirish bo‘yicha chora-tadbirlar yoki choralar ko‘rishi shart.

Texnologik (texnik) tadbirlar

83. Bank axborot xavfsizligini ta’minlash bo‘yicha texnologik (texnik) chora-tadbirlar quyidagilarga qaratilgan:

himoya qilish obyektlarining ishonchli, barqaror va xavfsiz ishlashini ta'minlash;

himoya qilinadigan obyektlarning uzluksiz ishlashini buzishdan himoya qilish;

tashqi muhit ta'siridan, tabiiy ofatlar va favqulodda vaziyatlardan himoya qilish obyektlarining xavfsizligi;

avariya vaziyatlarda himoya qilish obyektlarining faoliyatini operativ tiklash;

himoya qilinadigan obyektlarni foydalanishdan chiqarish jarayonida axborot xavfsizligini ta’minlash;

xodimlarga berilgan huquq va vakolatlar doirasida xatolik va huquqbuzarliklarga yo'l qo'yish ehtimolini kamaytirish.

84. Bankda qo‘riqlash obyektlarining barqaror va uzluksiz ishlashi uchun quyidagi chora-tadbirlar amalga oshiriladi:

a) uskunaning doimiy mavjudligi va yaxlitligini ta'minlash uchun tegishli texnik xizmat ko'rsatish (funksional monitoring, profilaktik xizmat ko'rsatish, ta'mirlash);

b) uskunani ochish, ta'mirlash, ishga tushirish, zaxira nusxasini yaratish, konfiguratsiyani o'zgartirish va hokazo kabi amaliy jarayonlarni hujjatlashtirish;

c) uskunalar va tizimlarning tizim jurnallarini boshqarish va tekshirish;

d) ishlamay qolishi nosozliklar va xavfsizlik buzilishiga olib kelishi mumkin bo'lgan axborotni qayta ishlash vositalari va tizimlaridagi o'zgarishlarni to'g'ri

boshqarish;

e) imkoniyatlarni boshqarish - kelajakdagi quvvatlarni rejalashtirish yoki prognoz qilish, resurslardan foydalanishni kuzatish, resurslar yoki qo'shimcha quvvatlarni zaxiralash;

f) ishlab chiqish, sinovdan o'tkazish va foydalanish muhitini ajratish - ishlab chiqish va sinov ishlari ishlaydigan tizimlardan alohida uskunalarda amalga oshirilishi kerak;

g) axborotni qayta ishlash, saqlash, uzatish va himoya qilish vositalarining ortiqchaligi;

h) ma'lumotlar va dasturiy ta'minotning zaxira nusxasini yaratish;

i) dasturiy ta'minotni boshqarish - dasturiy ta'minotni o'rnatish, o'zgartirish, sozlash va yangilash;

j) axborotni qayta ishlash obyektlari yaqinida ovqatlanish, ichish va chekish qoidalarini belgilash.

85. Bankning quyidagi texnik vositalari zaxira qilinadi:

bank axborot tizimlari serverlari (ma'lumotlar bazalari va ilovalari);

asosiy ma'lumotlarni qayta ishlash markazi va bosh ofisni (zaxira ma'lumotlarni qayta ishlash markazi) bank korporativ tarmog'iga va tashqi tarmoqlarga ulash uchun asosiy kommutatorlar va marshrutizatorlar;

asosiy ma'lumotlarni qayta ishlash markazi va bosh ofisni (zaxira ma'lumotlarni qayta ishlash markazi) bank korporativ tarmog'iga va tashqi tarmoqqa ulash chegaralarida foydalaniladigan tarmoqlararo ekran.

86. Bankda axborotni qayta ishlash, saqlash, uzatish va muhofaza qilish vositalarini, shuningdek aloqa kanallarini zaxiralashga qo'yiladigan talablar siyosatning 17-ilovasi "Favqulodda vaziyatlarda ish faoliyatini tiklashni va uzluksiz ishlashni ta'minlash rejasi"da belgilangan.

87. Aloqa kanallari zaxiralash, shuningdek, axborotni qayta ishlash, saqlash, uzatish va himoya qilish bo'yicha talablar Favqulodda (avariya) vaziyatlarida ish faoliyatini tiklash va uzluksiz ishlashni ta'minlash ushbu siyosatning 6-ilovasida keltirilgan Tizimli va amaliy dasturlarni yangilash, shuningdek ma'lumotlarni zaxira nusxalarini shakllantirish va tiklash to'g'risidagi nizomga muvofiq amalga oshiriladi.

88. Ma'lumotlarni zaxiralashni ta'minlash uchun ma'lumotlarni zaxiralash va qayta tiklash tizimlari orqali amalga oshiriladi.

89. Bank faoliyati uzluksizligi (elektr, telekommunikatsiya ta'minotidagi uzilish va nosozliklar, yordamchi xizmatlar - suv hamda gaz ta'minoti, kanalizatsiya, ventilyatsiya, havoni tozalash) tahdidlaridan himoya qilish uchun quyidagi choralar qo'llaniladi:

a) turli yo'nalishlar bo'ylab yotqizilgan bir nechta elektr ta'minoti liniyalariga ulanish;

b) dizel generatorlari, uzluksiz quvvat manbalaridan foydalanish;

c) bir nechta telekommunikatsiya marshrutlaridan foydalanish orqali aloqa kanallari va tarmoq ulanishlarining zaxira bo'lishi;

d) avariya sodir bo'lgan taqdirda suv ta'minoti, gaz ta'minoti va boshqa yordamchi xizmatlarni o'chirish uchun favqulodda quvvat kalitlari va klapanlardan foydalanish;

e) qurilmalar va jihozlarni yerga ulash va boshqalar.

90. Bankda uzluksiz elektr ta’minotini ta’minlash maqsadida quyidagilar amalga oshirilgan:

bank bosh ofis (AB va zaxira ma’lumotlarni qayta ishlash markazi) va Toshkent shahar MBXO (bosh ma’lumotlarni qayta ishlash markazi) binolarida dizel generatorlari;

bankda asosiy va zaxira ma’lumotlarni qayta ishlash ishlash markazidagi uskunalarni uzluksiz elektr energiyasi bilan ta’minlash uchun uzluksiz quvvat manbalari;

server va tarmoq uskunalarini uzluksiz quvvat bilan ta'minlash uchun uzluksiz quvvat manbalari, asosiy va zaxira ma'lumotlarni qayta ishlash markazlarining server xonasida (server raflari), shuningdek bank MBXO va BXM server xonalarida joylashgan axborotni himoya qilish vositalari va kompyuter texnikasi.

Shuningdek, bosh bank (AB va zaxira ma’lumotlarni qayta ishlash markazi) va Toshkent shahar MBXO (asosiy ma’lumotlarni qayta ishlash markazi) binolariga ikkita elektr tarmog‘ini yetkazib berish ko‘zda tutilgan.

91. Bosh ofisning ma'lumotlarni qayta ishlash markazidagi (AB va zaxira ma'lumotlarni qayta ishlash markazi) va asosiy ma'lumotlarni qayta ishlash markazini tashqi tarmoq va korporativ tarmoqqa ulash uchun foydalaniladigan aloqa kanallari, shuningdek, Bosh ofis, MBXO va BXMni asosiy tarmoqqa ulash uchun foydalaniladigan korporativ tarmoq kanallari zahiralanishi taminlanish zarur.

92. Bank tashqi muhit ta’siridan, tabiiy ofatlar va favqulodda vaziyatlardan (yong‘in, suv toshqini, zilzila, portlash, fuqarolik tartibsizliklari, tabiiy yoki texnogen oqibatlarning boshqa shakllari) himoya qilish bo‘yicha quyidagi chora-tadbirlarni amalga oshiradi:

a) ma'lumotlarni qayta ishlash markazining server xonalari MBXO va BXM server xonalaridagi axborotni qayta ishlash vositalarining ishlashiga salbiy ta'sir ko'rsatishi mumkin bo'lgan harorat, namlik va boshqalar kabi atrof-muhit sharoitlarini monitoring qilish;

b) server xonalarida talab qilinadigan iqlim sharoitlarini saqlash vositalaridan foydalanish (konditsionerlar);

c) xavfli yoki yonuvchan materiallarni himoyalangan hududdan yetarlicha masofada xavfsiz saqlashni ta'minlash;

d) yong'in signalizatsiyasi tizimlari va vositalari va yong'inga qarshi vositalardan foydalanish, shuningdek ularni tegishli joylarga joylashtirish;

e) yong'in sodir bo'lganda favqulodda chiqish joylarini jihozlash, evakuatsiya rejalarini ishlab chiqish;

f) loyihalash, qurish va kapital ta'mirlashda sanitariya va yong'in xavfsizligi standartlariga rioya qilish;

g) asosiy ma'lumotlarni qayta ishlash markazidan geografik jihatdan uzoqda joylashgan zaxiraviy ma'lumotlarni qayta ishlash markazida muhim axborot tizimlari va resurslari uchun zaxira uskunalarini joylashtirish.

93. Bank Bosh ofis, AB, MBXO, BXM binolarining asosiy binolariga yong‘in signalizatsiya tizimlari o‘rnatildi. Asosiy va zaxira ma'lumotlarni qayta

ishlash markazlarining server xonalarida avtomatik gazli yong'inni o'chirish tizimlari qo'llaniladi.

94. Asosiy va zaxiraviy ma’lumotlarni qayta ishlash markazining normal ishlashini ta’minlash uchun ular O‘zDSt 2875: 2014 “Ma’lumotlar markazlariga qo‘yiladigan talablar” talablariga javob berishi kerak. Infratuzilma va axborot xavfsizligini ta’minlash”.

95. Qayta tiklash choralariga quyidagilar kiradi:

a) tiklanish rejalarini tayyorlash, o'qitish va sinovdan o'tkazish;

b) avariya sodir bo'lgan taqdirda zaxira uskunalarini, aloqa kanallarini, liniyalarni yoki elektr ta'minoti manbalarini ishga tushirish;

c) dasturiy ta'minot va ma'lumotlarni zaxiradan tiklash;

d) uskunani ta'mirlash yoki almashtirish;

e) dasturiy ta'minotni qayta ishga tushirish yoki qayta o'rnatish va hokazo.

Axborotni qayta ishlash, saqlash, uzatish va muhofaza qilish vositalarini, shuningdek aloqa kanallarini zaxiralashga qo’yiladigan talablar siyosatning 17-ilovasi “Favqulodda vaziyatlarda ish faoliyatini tiklashni va uzluksiz ishlashni ta’minlash rejasi”da belgilangan.

96. Axborot xavfsizligini ta'minlash uchun himoya qilish obyektlarini foydalanishdan chiqarishda yoki axborotni qayta ishlashni yakunlash to'g'risida qaror qabul qilingandan so'ng, saqlash vositalaridan ma'lumotlarni va har qanday qoldiq ma'lumotlarni yo'q qilish (xavfsiz o'chirish) choralarini ko'rish va (yoki) ularni jismoniy zararsizlantirish choralarini ko'rish kerak. Bank boshqaruvi bilan kelishilgan holda saqlash vositalarini yo‘q qilish.

97. Ma'lumotlarni saqlash vositalari va qoldiq ma'lumotlarni yo'q qilish (xavfsiz o'chirish) va (yoki) ularni o'chirish paytida saqlash vositalarini jismonan yo'q qilish, siyosatning 9-ilovasiga (Mobil, ma’lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo’yicha yo‘riqnoma) muvofiq amalga oshiriladi.

98. Hujjatlashtirilgan konfidensial ma'lumotlar maxsus qirg'inchi (shredder) yordamida yo'q qilinishi kerak.

99. Axborotni qayta ishlash, saqlash, uzatish va himoya qilish vositalariga texnik xizmat ko'rsatuvchi xodimlar tomonidan xatolarga yo'l qo'ymaslik uchun ularning xatti-harakatlari hodisalar jurnallarini tahlil qilish orqali nazorat qilinishi kerak. Ushbu tahlil bank Axborot texnologiyalari departamenti mas’ul xodimi tomonidan amalga oshirilmoqda.

Muhandis-texnik choralar

100. Muhandis-texnik tadbirlar himoya qilinadigan obyektlarga ruxsatsiz shaxslarning kirishi uchun jismoniy kirishni oldini olish yoki to’siqlar yaratishga qaratilgan va quyidagi tadbirlarni o’z ichiga oladi:

1) 1 zonali, 2 zonali va 3 zonali eshiklar va boshqa muhandislik vositalar o'rtasida kirishni boshqarish;

2) 2 zonaga kirishda va 3 zonali xonalarga kirishda kodli qulflarni, ushbu binolarga kirish huquqiga ega bo'lgan xodimlar uchun identifikatsiyalash plastik kartalaridan foydalangan holda va biometrik identifikatsiyalash (yuz va / yoki barmoq izini aniqlash) bilan orqali aniqlaydigan qulflarni o'rnatish;

3) 3-zona xonalarga kirishda temir eshiklardan foydalanish;

4) binolarning derazalarini vizual kuzatishdan himoya qilish vositalari bilan jihozlash (pardalar, jalyuzalar);

5) Bank binolarining perimetri, kirish qismi va koridorlarini, shuningdek bank binosining 3-zonasi binolarini videokuzatuvdan o‘tkazish uchun videokuzatuv tizimidan foydalanish;

6) Bankomatlarda videokuzatuvdan foydalanish;

7) himoyalangan binolarga ruxsatsiz jismoniy kirish faktlarini qayd etish uchun qo'riqlash signalizatsiyasi va datchiklarni o'rnatish;

8) hujjatlashtirilgan konfidensial ma'lumotlarni va konfidensial ma'lumotlarni tashuvchilarini saqlash uchun qulflanadigan temir yong'inga qarshi shkaflardan foydalanish;

Dasturiy-apparat choralari

101. Bankning axborot xavfsizligini ta’minlash bo’yicha apparat-dasturiy choralar quyidagilarga qaratilgan:

axborotni texnik muhofaza qilishni tashkil etish;

axborotning kriptografik himoyasini tashkil etish.

102. Axborotni texnik muhofaza qilishni ta’minlash uchun axborotni quyidagi texnik muhofaza qilish vositalari qo’llaniladi:

tarmoqlararo ekranlar;

DLP vositalari;

virusga qarshi himoya vositalari;

kirishni boshqarish vositalari va boshqalar.

konfidensial ma’lumotlarni chiqib ketishini oldini olish vositasi;

xavfsizlikni kuzatish va tahlil qilish vositalari, shuningdek axborot xavfsizligi hodisalarini boshqarish hamda monitoring qilish va boshqalar.

103. Tarmoq xavfsizligi choralariga quyidagilar kiradi:

a) Bank tarmoq infratuzilmasining xavfsiz arxitekturasini aniqlash;

b) Bank tarmoqlarini jismoniy va virtual jihatdan ajratish;

c) Bankda tarmoq xavfsizligi vositalaridan (faervollar, IDPS tizimlari, VPN vositalari) foydalanish;

d) xavfsiz kanallar va tarmoq ulanishlarini tashkil etish.

104. Bank korporativ tarmog‘ining xavfsiz arxitekturasi, uni qurish tamoyillari, shuningdek, xavfsiz kanallar va tarmoq ulanishlarini tashkil etish siyosatning 1- ilovasida keltirilgan Korporativ tarmoq va xavfsiz tarmoq ulanishlarini tashkil etish to‘g‘risidagi nizomda belgilangan.

105. Tarmoq infratuzilmasi xavfsizligini ta’minlash va tarmoqlararo ekranlardan foydalanish, siyosatining 2-ilovasida keltirilgan Tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta’minlash to’g’risida nizomga muvofiq amalga oshiriladi.

106. Bank axborot resurslari va tizimlaridan foydalanishni farqlash uchun siyosatning 10-ilovasida keltirilgan Axborot resurslariga kirish matritsasini ishlab chiqish qoidalariga muvofiq foydalanish matritsasi ishlab chiqilgan.

107. Bankda himoyalangan obyektlarga kirishda foydalanuvchilarning autentifikatsiyasi parollar va boshqa identifikatorlar, siyosatining 7-ilovasida keltirilgan Parol bilan himoya qilish va foydalanuvchilarni axborot tizimiga autentifikatsiyasi bo‘yicha yo‘riqnoma muvofiq ishlab chiqariladi va foydalaniladi.

108. Bankda virusga qarshi himoya qilish uchun quyidagi virusga qarshi himoya choralari va vositalari qo‘llaniladi:

a) ma'lumotlarni qayta ishlash vositalarida, shu jumladan mobil qurilmalarda ularni aniqlash va blokirovka qilishni, asl holatini tiklashni ta'minlaydigan, shuningdek foydalanuvchilarni xabardor qilish uchun mo'ljallangan zararli dasturlardan (antiviruslardan) foydalanish;

b) Bankda bank xodimlari tomonidan bajarilishi kerak bo‘lgan zararli dasturlardan himoyalanish talablarini belgilovchi virusga qarshi himoya siyosatini qabul qilish;

c) zararli dasturlardan foydalanish mumkin bo'lgan zaifliklarni aniqlash va yo'q qilish;

d) axborotni qayta ishlash vositalarida USB portlaridan foydalanishni bloklash.

109. Jarayonlar, shu jumladan virusga qarshi himoyani tashkil etish va ta'minlash, xodimlar tomonidan zararli dasturlardan himoya qilish talablarini belgilash va bajarish tartibi siyosatning 8-ilovasiga muvofiq antivirus himoya qilish bo'yicha yo'riqnomada belgilangan.

110. Bank xavfsizlikni monitoring qilish va tahlil qilish vositasi sifatida aloqa kanallari, asosiy serverlar va tarmoq uskunalari faoliyati holatini monitoring qilish tizimidan, shuningdek, xavfsizlikni monitoring qilish va tahlil qilish vositalaridan (zaifliklar skanerlari) foydalanadi.

111. DLP tizimi konfidensial ma'lumotlarning chiqib ketishidan himoya qilish vositasi sifatida ishlatiladi.

Shuningdek, ruxsat etilmagan harakatlar va axborot tizimlari ma’lumotlar bazalaridan ma’lumotlarning chiqib ketishi faktlarini aniqlash maqsadida bank tezkor xotiradan imtiyozli foydalanuvchilarni nazorat qilish tizimidan foydalanadi.

112. Bankda qo’llaniladigan axborotni texnik muhofaza qilish usullari va vositalari, siyosatining 14-ilovasidagi Axborotni texnik himoya qilishni tashkil etish bo’yicha yo’riqnomada keltirilgan.

113. Bankda ma’lumotlarni kriptografik himoya qilish axborotni kriptografik himoyalash vositalaridan (keyingi o‘rinlarda AKH deb yuritiladi) foydalangan holda tashkil etiladi.

114. Bankda AKH ma’lumotlarning muallifligi va yaxlitligini ta’minlash maqsadida elektron raqamli imzoni (keyingi o‘rinlarda – ERI deb yuritiladi) shakllantirish va tekshirish shuningdek, ERI asosida ABT foydalanuvchilari bo‘lgan bank xodimlarining autentifikatsiyasini amalga oshirish uchun qo‘llaniladi.

ERI mablag'lari bankning yuridik shaxs bo'lgan mijozlari tomonidan Internet-Banking va mobil Banking xizmatlaridan foydalanganda ERIni yaratish va tasdiqlash uchun foydalaniladi.

115. ERIdan ABT tizimida shuningdek, internet-Banking va mobil Banking mijozlari tomonidan foydalanish uchun bank ERI kalitlarini ro‘yxatga olish markazi tomonidan ishlab chiqarilgan ERI yopiq kalitlari va ERI ochiq kalitlari sertifikatlaridan foydalaniladi.

116. Bank O’zbekiston Respublikasi Prezidentining 2007 yil 3 apreldagi PQ-614-sonli farmoniga binoan kriptografik ma’lumotlarni himoya qilish vositalari uchun sertifikatlash organi tomonidan sertifikatlangan AKHVdan foydalanishi

shart.

117. Bankda axborotni kriptografik himoyalash usullari va vositalari, siyosatining 15-ilovasida keltirilgan Axborotni kriptografik himoya qilishni tashkil etish bo'yicha yo'riqnomaga muvofiq amalga oshiriladi.

Tashqi foydalanuvchilar bilan ishlashda xavfsizlik choralari

118. Bank axborot aktivlarini himoya qilish uchun uchinchi tomon tashkilotlari bilan o'zaro hamkorlik qilish va mijozlar bilan ishlashda axborot xavfsizligini ta'minlash choralari qo'llanilishi, ular kirish yoki olishi mumkin.

Shu bilan birga, uchinchi tomon tashkilotlari yoki mijozlari bank axborot aktivlariga ham jismoniy, ham mantiqiy ruxsat olishlari mumkin.

Bank bunday ruxsatni olish imkoniyatini taqdim etish orqali axborot xavfsizligining buzilishi yoki zaiflashishiga olib kelishi mumkinligini biladi.

119. Axborot xavfsizligi choralari uchinchi shaxslar bilan o'zaro munosabatlarning quyidagi hollarda ko'rib chiqiladi:

a) uchinchi shaxs (pudratchilar, yetkazib beruvchilar va boshqalar) tomonidan xizmatlar ko'rsatish yoki ishlarni bajarishdagi munosabatlar;

b) bank axborot tizimining uchinchi tomon tashkilotining axborot tizimi bilan o'zaro hamkorligi;

c) bank axborot tizimiga uchinchi tomon tashkiloti xodimlarini ulash va ulardan foydalanish imkoniyatini ta'minlash;

d) tashqi tashkilotlar vakillarini qabul qilish va ular bilan uchrashuvlar o'tkazish.

120. Mijozlar bilan ishlashda axborot xavfsizligi choralari ular bilan bevosita aloqada bo'lish (oflayn xizmat) orqali xizmat ko'rsatilayotgan mijozlar bilan ishlashda alohida va interaktiv bank xizmatlaridan foydalanuvchi mijozlar bilan (onlayn xizmat) alohida belgilanadi.

121. Bank xizmatlar ko'rsatuvchi va ishlarni amalga oshiruvchi begona tashkilotlar bilan o'zaro hamkorlikda axborot xavfsizligini ta'minlash bo'yicha quyidagi choralarni ko'radi:

a) Bank obyektlari bilan shartnoma tuzishdan oldin uning ishlashi va himoya qilinishiga ruxsat berilgan uchinchi shaxs tashkiloti va uning mutaxassislariga qo'yiladigan talablarni belgilash;

b) uchinchi shaxslar bilan tuzilgan shartnoma shartlariga axborot xavfsizligi talablarini kiritish;

c) uchinchi shaxslar bilan qo'shimcha konfidensial shartnomalarini tuzish yoki ularni shartnoma shartlariga kiritish;

d) xizmatlar ko'rsatish yoki ishlarni bajarishda uchinchi tomon tashkiloti kirish huquqiga ega bo'lgan ma'lumotlar va himoya obyektlari ro'yxatini, shuningdek uchinchi tomon tashkilotining bunday kirish huquqiga ega bo'lgan shaxslar ro'yxatini tuzish;

e) kirish turlari va kirish tartibini ko'rsatgan holda uchinchi shaxs tomonidan ruxsat olish uchun ruxsat olish tartiblarini belgilash;

f) Bank axborot xavfsizligi talablarini ish olib borilgunga qadar uchinchi tomon tashkiloti mutaxassislariga yetkazish;

g) uchinchi shaxsga axborot va himoyalangan obyektlarga kirish huquqini berishdan oldin tegishli choralar va nazorat qilish va boshqarish vositalarini (jismoniy yoki mantiqiy) ko'rish;

h) Bank boshqaruvidagi axborotni qayta ishlash vositalarini uchinchi shaxs tomonidan boshqariladigan axborotga ishlov berish vositalaridan jismoniy ajratish;

i) uchinchi tomon tashkilotining axborotni himoya qilish, qayta ishlash va uzatish obyektlariga kirishini nazorat qilish, shuningdek ushbu kirishni kuzatish va boshqarish;

j) Bank xodimining qo‘riqlash obyektida uchinchi tomon tashkiloti tomonidan ishlarni bajarayotganda doimiy bo‘lishi;

k) Bank xodimiga ma’lum bo‘lgan himoyalangan obyektga imtiyozli foydalanish huquqlarini istisno qiluvchi yagona kirish identifikatorlarini uchinchi tomon tashkilotiga taqdim etish;

l) uchinchi tomon tashkiloti tomonidan ish tugagandan so'ng kirish huquqlarini bekor qilish, ma'lumotlarning yaxlitligini tekshirish, uskunalarini sozlash;

m) uchinchi shaxsga tegishli bo'lgan mablag'lardan foydalanish va joylashtirishni muvofiqlashtirish.

Yuqoridagi chora-tadbirlar, shuningdek ularni amalga oshirish tartibi va bankning axborot xavfsizligiga oid boshqa talablari uchinchi tomon tashkiloti bilan tuzilgan shartnomada belgilanadi.

122. Uchinchi tomon tashkiloti bilan tuzilgan konfidensiallik shartnomasi uchinchi tomon tashkilotining konfidensial ma'lumotlarni oshkor qilmaslik bo'yicha majburiyatlarini va uchinchi tomon tashkilotining ushbu ma'lumot uning aybi bilan oshkor qilingan taqdirda javobgarligini, Bankka ushbu ma'lumotlar oshkor etilishi natijasida yetkazilgan zararni qoplashni belgilaydi.

Konfidensiallik to'g'risidagi shartnoma shartlari amal qilish muddati davomida va u bekor qilinganidan keyin kamida 5 yil davomida bajarilishi kerak.

123. Bank axborot tizimi uchinchi tomon tashkilotining axborot tizimi bilan o‘zaro aloqada bo‘lganda yoki uchinchi tomon tashkiloti xodimlariga bank axborot tizimiga kirishini ta’minlashda axborot xavfsizligini ta’minlash bo‘yicha quyidagi choralar qo‘llaniladi:

a) axborot tizimini yoki uchinchi tomon tashkilotining xodimlarini ulashda axborot xavfsizligi talablarini belgilash;

b) Bank tomonidan uchinchi tomon tashkilotining uning axborot tizimiga ruxsatsiz mantiqiy kirishini istisno qiladigan chora-tadbirlar va vositalarni ko‘rish;

c) axborot almashinuvi uchun xavfsiz ulanishlarni tashkil etish va boshqalar.

Yuqoridagi choralar ikki tomonlama shartnomalarda belgilangan.

Xavfsiz ulanishlarni tashkil etish siyosatning 1-ilovasiga muvofiq korporativ tarmoq va xavfsiz tarmoq ulanishlarini tashkil etish to‘g‘risidagi nizom talablariga muvofiq amalga oshiriladi.

Uchinchi tomon tashkilotlari va ularning axborot tizimlarini bank axborot tizimlariga ulashda siyosatning 2-ilovasiga muvofiq tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta’minlash to‘g‘risidagi nizomga muvofiq tarmoqlararo ekran choralari qo‘llanilishi kerak.

124. ABT uchinchi tomon axborot tizimlari bilan o'zaro aloqada bo'lganda,

quyidagi choralar ko'riladi:

1) ABT ni uchinchi tomon tashkilotlarining axborot tizimlariga ulash Markaziy bankning BTS orqali amalga oshiriladi;

2) uchinchi tomon tashkilotlarining axborot tizimlari bilan o'zaro aloqa qilish uchun ABT ni tashqi kanallarga ulash tarmoqlararo ekran va IDPS vositalari orqali amalga oshiriladi;

3) ABT tashqi axborot tizimlariga ulanganda xavfsiz IPSec VPN kanallari tashkil qilinadi.

125. Uchinchi tomon tashkilotlar vakillarini qabul qilish va ular bilan uchrashuvlar o‘tkazishda bank tomonidan ularning bankning qo‘riqlash vositalariga ruxsatsiz jismoniy kirishiga yo‘l qo‘ymaslik bo‘yicha quyidagi choralar ko‘riladi:

a) qabulxonalarda (majlislar zali) yoki bank hududlaridan uzoqda joylashgan maxsus xonalarda vakillarni qabul qilish va ular bilan uchrashuvlar o‘tkazish;

b) bank xodimlari tomonidan vakilni bino ichida kuzatib borish;

c) bank tarmog‘iga yoki axborot tizimlariga ulangan ish stansiyalarida vakilga ishlash huquqini berish, shuningdek, ularning qurilmalarini bank tarmog‘i va axborot tizimlariga ulash bo‘yicha cheklovlar belgilash;

126. Mijozlar bilan ishlashda quyidagi axborot xavfsizligi choralari ko'riladi:

a) bevosita mijozlarga xizmat ko'rsatishda:

bank mijozlarga faqat 1-zonada va yuqori xavfsizlik zonalaridan uzoqda joylashgan boshqa binolarda xizmat ko‘rsatish;

mijozlarning bank ichki ofis binolariga kirish imkoniyatini istisno qilish;

bank xizmatlaridan foydalanishda mijozning axborot xavfsizligi masalalari bo‘yicha majburiyatlari va javobgarliklari yoki bank mijozga foydalanish uchun taqdim etilgan aktivlarini himoya qilish tartib-qoidalari bilan tushuntirish yoki tanishtirish;

b) Bankning interaktiv bank xizmatlaridan foydalanuvchi mijozlarga nisbatan:

internet-banking va mobil bankingdan foydalanishda mijoz tomonidan axborot xavfsizligi talablarini belgilash va bajarish;

bank va mijozlar o‘rtasidagi interaktiv bank xizmatlaridan foydalanishda javobgarlikni chegaralash;

foydalanuvchilarga ruxsat berilgan kirish usullarini taqdim etish, shuningdek, noyob foydalanuvchi identifikatorlari va parollarini boshqarish va ulardan foydalanish;

foydalanuvchi tomonidan axborot xavfsizligi talablari buzilgan taqdirda foydalanish huquqini bekor qilish;

foydalanuvchilarni interaktiv bank xizmatlaridan foydalanishda axborot xavfsizligi talablarini buzgan taqdirda yuzaga keladigan xavflar bilan tanishtirish.

Ushbu xavfsizlik talablari va ularga rioya qilmaslik mijozlar bilan tuzilgan shartnomalarda ko’rib chiqiladi.

127. Uchinchi tomon tashkilotlari bilan o‘zaro munosabatlarda va mijozlar bilan ishlashda axborot xavfsizligini ta’minlash choralarini ta’minlashga qo‘yiladigan talablar Xavfsizlik va axborotlarni muhofaza qilish departamenti

tomonidan belgilanadi hamda mazkur talablarning bank tarkibiy bo‘linmalari va xodimlari tomonidan bajarilishini nazorat qiladi.

IX. Axborot xavfsizligi hodisalariga munosabat bildirish

128. Bank integratsiyalashgan AXBT tizimidagi muhim jarayonlardan biri axborot xavfsizligi hodisalarini boshqarish jarayonidir.

129. Bank axborot xavfsizligi hodisalarini boshqarishda izchil, samarali va tizimli yondashuvni qo‘llashi kerak.

130. Bankda axborot xavfsizligi hodisalarini boshqarish maqsadlari quyidagilar:

bankka axborot xavfsizligi hodisalari natijasida yetkazilgan yo‘qotishlar va zararlarni minimallashtirish;

hodisalarni mahalliylashtirish, tahdidlarning oldini olish va ularning oqibatlarini imkon qadar qisqa muddatlarda bartaraf etish uchun tezkor va samarali choralar ko‘rish;

hodisalardan saboq olish, ularning takrorlanish xavfini kamaytirish yoki kelajakda ularni oldini olish;

bank va uning faoliyati uchun hodisalarning salbiy oqibatlarini minimallashtirish;

inqirozni boshqarish va biznesning uzluksizligini boshqarishning tegishli elementlari bilan kuchayish;

axborot xavfsizligi zaifliklarini baholash va ushbu zaifliklar bilan bog'liq hodisalar sonini oldini olish yoki kamaytirish uchun tegishli tarzda chora ko’rish.

Bankda axborot xavfsizligi hodisalarini boshqarishning belgilangan maqsadlari axborot xavfsizligi insidentlarini boshqarishga mas’ul bo‘lgan xodimlar e’tiboriga bankning hodisalarga javob berishda ustuvor yo‘nalishlarini yetkazilishi kerak.

131. Bank axborot xavfsizligi hodisalarini boshqarish bo‘yicha quyidagi tartiblarni qo‘llashi lozim:

1) hodisalarni kuzatish va aniqlash;

2) hodisalarni tahlil qilish, baholash va hisobot berish;

3) hodisalarni hisobga olish va ro'yxatga olish;

4) hodisalar to'g'risida xabar va ma'lumot berish;

5) tahdidni mahalliylashtirish yoki hodisaga olib kelgan tahdidning harakatini bartaraf etish;

6) hodisa oqibatlarini baholash;

7) voqea sodir bo'lganidan keyin tiklanish va uning oqibatlarini bartaraf etish;

8) hodisani tahlil qilish va hodisa sabablarini aniqlash;

9) hodisalarning takrorlanishining oldini olish bo'yicha chora-tadbirlarni ishlab chiqish va qabul qilish;

10) dalillarni to'plash, tahlil qilish va saqlash, tergov o'tkazish;

11) hodisaning sabablari va oqibatlari uchun javobgar shaxslarni javobgarlikka tortish.

132. Siyosatning 8-bo'limida belgilangan barcha himoya obyektlari monitoring qilinadi.

Monitoring axborot xavfsizligi hodisalarini aniqlash maqsadida amalga oshiriladi va tunu - kun amalga oshiriladi.

Himoya qilinadigan obyektlardagi axborot xavfsizligi hodisalari to'g'risidagi ma'lumotlar manbalari:

axborot xavfsizligi monitoringi va hodisalarni boshqarish tizimining ma'lumotlari (keyingi o'rinlarda SIEM tizimi deb yuritiladi);

korporativ tarmoqning tarmoq uskunalari, axborot tizimlari va boshqa muhim uskunalar uchun axborotni qayta ishlash vositalarining ishlashini monitoring qilish tizimining ma'lumotlari shuningdek, so'rovlar va bank resurslarining yuklanishi monitoringi (keyingi o'rinlarda Zabbix tizimi deb yuritiladi);

Elastics Logstasch Kibana dasturiy ta'minoti (keyingi o'rinlarda ELK tizimi) asosida qurilgan Bankda tarmoqlararo ekrandan tizim jurnallari (jurnal fayllari) ma'lumotlarini yig'ish va qayta ishlash tizimining ma'lumotlari;

axborot tizimlari, uskunalari va dasturiy ta'minotining tizim jurnallari (log fayllari) ma'lumotlari;

axborot xavfsizligi vositalarining chiqish ma'lumotlari;

bank korporativ va lokal tarmoqlari uskunalari va tarmoq obyektlari, axborot resurslari va axborot tizimlarining sog'lom holatini vizual nazorat qilish;

axborot xavfsizligining ichki yoki tashqi auditi natijalari;

bank xodimlariga ma'lumot yoki xabar berish;

bank mijozlari va bank bilan o'zaro hamkorlik qiluvchi tashqi tashkilotlarning shikoyatlari;

o'g'irlik, hujumlar, sizib chiqish va ruxsatsiz ulanish va boshqa faktlarini aniqladi.

133. Axborot xavfsizligi hodisalarini kuzatish va aniqlash uchun bank axborot xavfsizligi hodisalarini monitoring qilish va boshqarish tizimlaridan foydalanadi.

134. Bank xodimlari monitoringni, Xavfsizlik va axborotlarni muhofaza qilish departamenti, bank Axborot texnologiyalari departamenti, MBXO Xavfsizlik va axborotni muhofaza qilish bo'limi hamda MBXO Axborot texnologiyalari bo'limlari xodimlari tomonidan amalga oshiriladi.

135. Axborot xavfsizligi hodisasini tahlil qilish va baholash, axborot xavfsizligi hodisasi sifatida tasniflash kerakmi yoki yo'qligini hal qilish, shuningdek hodisaning jiddiylik darajasini aniqlashni amalga oshiriladi.

136. Bankda sodir bo'lgan axborot xavfsizligini ta'minlash bo'yicha quyidagi hodisalar deb hisoblanishi kerak:

1) favqulodda va avariya vaziyatlar (texnogen tahdidlar, tabiiy ofatlar, ommaviy namoyishlar va boshqalar);

2) Bank axborot tizimlarining ishlashi va ishlashidagi nosozliklar - server va tarmoq uskunalari, dasturiy ta'minotdagi nosozliklar;

3) Bank konfidensial ma'lumotlarining konfidensial, yaxlitligi va mavjudligini buzish – konfidensial ma'lumotlarni himoya qilish talablarini buzish;

4) o'g'irlik, sizib chiqish va moddiy zarar yetkazish bo'yicha boshqa ruxsat etilmagan harakatlar - qimmatbaho moddiy boyliklar, mablag'lar va konfidensial ma'lumotlarni yo'qotish va o'g'irlash faktlari;

5) tashqi tarmoqlar bilan aloqani yo'qotish, shuningdek uchinchi tomon axborot tizimlari bilan ma'lumot almashishni buzish;

6) bank korporativ tarmog‘ida, shuningdek, bosh ofis (AB), MBXO, BXMning lokal tarmoqlarida aloqa uzilishi, tarmoq uskunasining texnik nosozligi, kabelning uzilishi va boshqalar;

7) har qanday sababga ko'ra, texnik nosozlik natijasida ham, inson omili bilan bog'liq xatolar natijasida ham axborot xavfsizligi vositalarining ishdan chiqishi;

8) bank axborot tizimlari va resurslariga uchinchi shaxslarning ruxsatsiz jismoniy yoki mantiqiy kirishi;

9) DoS (Denial of Service) va DDoS (Distributed Denial of Service) xizmat ko‘rsatishni rad etish;

10) himoya vositalari bilan aniqlangan tarmoq hujumlari;

11) aniqlangan xavfli viruslar va zararli dasturlar;

12) qurilmalar, tarmoq uzellariga, korporativ va lokal tarmoqlarga ruxsatsiz ulash;

13) qo'riqlanadigan binolarga ruxsat etilmagan shaxslarning ruxsatsiz kirishi (3-zona);

14) ma'lumotlarni to'plash va olib tashlash bo'yicha noqonuniy harakatlar aniqlash.

137. Xavfsizlik va axborotlarni muhofaza qilish departamenti axborot xavfsizligi hodisalarini tahlil qilish va baholash, ularni hodisa sifatida tasniflash va ularning xavflilik darajasini aniqlash uchun hisoblanadi.

138. Bank bosh ofisida (AB), MBXO, BXM, masofaviy kassalarida sodir bo‘lgan barcha axborot xavfsizligi hodisalari ushbu bo‘limning 136-bandida ko‘rsatilgan ro’yxat bo’yicha hisobga olinishi lozim.

Aniqlangan axborot xavfsizligi hodisalarini hisobga olish axborot xavfsizligi hodisalarini monitoring qilish va boshqarish tizimlari tomonidan amalga oshiriladi. Axborot xavfsizligi monitoringi va hodisalarni boshqarish tizimlari tomonidan aniqlanmagan axborot xavfsizligi hodisalarini hisobga olish uchun axborot xavfsizligi hodisalarining alohida elektron ma’lumotlar bazasi yuritiladi. Xavfsizlik va axborotlarni muhofaza qilish departamenti bankda aniqlangan axborot xavfsizligi hodisalarini hisobga olish shuningdek, axborot xavfsizligi hodisalari to‘g‘risidagi elektron ma’lumotlar bazasini yuritish bilan shug‘ullanadi. Axborot xavfsizligi insidentlarining elektron ma’lumotlar bazasining shakli siyosatning 18-ilovasiga muvofiq “Axborot xavfsizligi hodisalariga javob choralari ko‘rish to‘g‘risida”gi nizomda keltirilgan.

139. Axborot xavfsizligi hodisalarini hisobga olish sabablarini aniqlash, voqeani tahlil qilish va bank axborot xavfsizligi risklarini baholash zarur.

140. Axborot xavfsizligining “yuqori” darajadagi xavfli hodisalari ro'yxatga olinishi kerak. Ushbu hodisalarni ro‘yxatga olish uchun ular to‘g‘risidagi ma’lumotlar bankning Favqulodda xavfsizlik holatlari reyestriga kiritiladi, uning shakli siyosatning 18-ilovasida keltirilgan.

Xavfsizlik va axborotlarni muhofaza qilish departamenti bankning “yuqori” xavflilik darajasidagi axborot xavfsizligi hodisalarini ro‘yxatga olish va favqulodda xavfsizlik holatlari jurnalini yuritish javobgardir.

141. Noxush hodisalar haqida ogohlantirish yoki xabardor qilish zarur bulganlar:

noxush hodisa oqibatida zarar ko‘rgan bankda ishlab chiqarish maydonchasi yoki texnologik jarayon uchun mas’ul tarkibiy bo‘linmalarni rahbarlari;

himoya obyektini saqlash uchun mas'ul bo'lgan tarkibiy bo'linma rahbariyati yoki mutaxassis (administrator);

bank rahbariyati;

tashqi manfaatdor tashkilotlar.

142. Hodisa sodir bo‘lgan tahdid zararni minimallashtirish, faoliyatini tiklashga o‘tish yoki bank tomonidan hodisa ta’sir ko‘rsatmaydigan boshqa vazifalar va jarayonlarning bajarilishini ta’minlash.

143. Hodisa oqibatlarini baholash natijasida yetkazilgan zararning ko'lamini, hodisa natijasida ko'rsatilgan yo'qotishlarni aniqlash kerak.

144. Tahdidni mahalliylashtirish yoki zararsizlantirishdan so'ng quyidagilarni amalga oshirish kerak:

faoliyatni tiklash va hodisa oqibatlarini bartaraf etish bo'yicha ishlar;

hodisani tahlil qilish;

hodisaning manbalari va sabablarini aniqlashtirish;

dalillarni to'plash.

145. Axborot xavfsizligi hodisasini tahlil qilishda quyidagilarni aniqlash kerak:

hodisaga olib kelgan tahdidlarning xususiyatlari, aniqlangan tahdid turlarining paydo bo'lish chastotasi;

hodisa sabablari va tahdid manbalari;

hodisa uchun zaifliklardan foydalanilganligi;

hodisalarni boshqarish va himoya qilish tizimidagi mavjud xato va kamchiliklar;

xodimlarning harakatlarining samaradorligini, hodisalarni boshqarishning tartiblari va jarayonlarini baholash.

146. Axborot xavfsizligi hodisalarini tahlil qilish natijalari va hodisadan olingan saboqlar kelajakda takrorlanishining oldini olish yoki shunga o'xshash hodisalar ehtimolini kamaytirish choralarini ishlab chiqish va chora ko'rish uchun ishlatilishi kerak.

Ushbu chora-tadbirlar kamchiliklarni bartaraf etish, samaradorlikni oshirish va zaifliklarni bartaraf etish, himoya qilish usullari va vositalarini takomillashtirishga qaratilgan bo'lishi kerak.

147. Tahdidni mahalliylashtirish va zararsizlantirish, hodisa oqibatlarini baholash, hodisa oqibatlarini tiklash va bartaraf etish, axborot xavfsizligi hodisasini tahlil qilish uchun bank axborot xavfsizligi hodisalariga qarshi kurashish guruhi mas’ul, uning tarkibi bank buyrug‘i bilan belgilanadi.

Zarur hollarda, bank rahbariyati bilan kelishilgan holda boshqa tarkibiy bo‘linmalarning yoki manfaatdor tashkilotlarning xodimlari ko‘rsatilgan hodisalarni bartaraf etish tartib-taomillariga jalb etilishi mumkin.

MBXO, BXM va ularga qarashli masofaviy kassalarda axborot xavfsizligi bilan bog‘liq hodisalar sodir bo‘lgan taqdirda, tahdidlarni mahalliylashtirish va zararsizlantirish jarayonlariga O‘zbekiston Respublikasi Markaziy banki Xavfsizlik va axborotni muhofaza qilish bo’limi hamda Axborot texnologiyalari bo‘limi xodimlari jalb etiladi. Hodisalarning oqibatlarini baholash shuningdek, hodisalar oqibatlarini tiklash va bartaraf etish.

148. Axborot xavfsizligi insidentlarini boshqarishda dalillarni to'plash sud va boshqa holatlar uchun dalil bo'lib xizmat qilishi va aybdorlarni javobgarlikka tortish yoki intizomiy jazo choralarini qo'llash uchun asos bo'lishi mumkin bo'lgan ma'lumotlarni aniqlash, to'plash, o'rgatish va saqlashga qaratilgan bo'lishi kerak.

149. Hodisalarni tekshirish jarayonida dalillar to'plash. Voqea yuzasidan surishtiruv o‘tkazish uchun bank rahbariyatiga tegishli tarkibidan iborat maxsus guruh tuziladi.

150. Axborot xavfsizligi hodisalarni boshqarish taomillarini amalga oshirish tartibi ushbu bo‘limning 131-bandida ko‘rsatilgan, hodisalarni bartaraf etish bo‘yicha mas’ul shaxslarning, shuningdek, hodisalarni boshqarish bo‘yicha bank xodimlarining majburiyatlari “Axborot xavfsizligi hodisalariga berish qoidalari siyosatning 18-ilovasida keltirilgan.

151. Axborot xavfsizligi hodisalarni boshqarishda bank quyidagi uchinchi tomon tashkilotlar bilan o‘zaro hamkorlik qilishi mumkin:

a) O‘zbekiston Respublikasi Markaziy banki (CERT-CBU) sodir bo‘lgan hodisalar, ko‘rilayotgan chora-tadbirlar va ularni amalga oshirishning borishi to‘g‘risida xabardor qilish nuqtai nazaridan;

b) “Kiberxavfsizlik markazi” davlat unitar korxonasi hodisalar to‘g‘risida xabardor qilish, ularni bartaraf etish oqibatlarini va takrorlanishining oldini olish bo‘yicha maslahat va tavsiyalar olish, berilgan tavsiyalarning bajarilishi yuzasidan hisobotlar taqdim etish;

c) Bank o‘z faoliyati davomida sodir bo‘lgan hodisalar to‘g‘risida xabardor qilish, oqibatlarini bartaraf etish va shunga o‘xshash hodisalarning takrorlanishining oldini olish bo‘yicha birgalikdagi chora-tadbirlarni ishlab chiqish bo‘yicha o‘zaro hamkorlik qiladigan manfaatdor uchinchi tomon tashkilotlari (hamkorlar, xizmat ko‘rsatuvchi tashkilotlar, yetkazib beruvchilar);

d) jinoyat ishlarini qo'zg'atish va hodisalarni tergov qilishda ishtirok etish nuqtai nazaridan huquqni muhofaza qilish organlarini jalb qilish;

e) favqulodda holatiga mas'ul organlar, hodisa oqibatida yuzaga kelgan hodisalar to'g'risida xabardor qilishi, ularning oqibatlarini bartaraf etishda ishtirok etish;

f) Bank mijozlariga nosozliklar haqida xabar berish va ularni bartaraf etish, kamchiliklarni bartaraf etish yoki xizmatlarni qayta tiklash to'g'risida xabardor qilish va boshqalar bo'yicha hamkorlik qilish.

152. Axborot xavfsizligi hodisalarini boshqarishda tashqi tashkilotlari bilan o'zaro hamkorlik qilish tartibi siyosatning 18-ilovasida keltirilgan.

X. Aloqa kanallarining xavfsizligini ta’minlash

153. Bankda ma’lumot uzatish uchun ishlatiladigan elektr va tarmoq

kabellari ma’lumotni o‘g‘irlash va buzilishining oldini olish uchun himoyalangan bo‘lishi kerak. Bankda ushbu xavfni kamaytirish uchun quyidagi himoya choralari qo‘llaniladi:

a) elektr va aloqa kabellari (imkon qadar) yer ostida, kanalizatsiya va kollektorlarda, binolar ichida bo‘lishi kerak yoki ruxsatsiz jismoniy kirishdan to‘g‘ri himoyalangan bo‘lishi kerak;

b) tarmoq kabellari, iloji boricha, bir-biriga salbiy ta'sir ko'rsatmaslik uchun elektr kabellaridan alohida yotqizilishi kerak;

c) tarmoq kabelini yotqizish marshruti jamoat joylarini chetlab o'tib tanlanishi kerak va bunday texnik imkoniyat bo'lmasa, tarmoq kabeli maxsus korpus yoki metall quti yordamida himoyalangan bo'lishi kerak;

d) foydalanilmagan tarmoq kabeli uchun mo'ljallangan tarmoq nuqtalari muhrlangan yoki maxsus marka bilan muhrlangan bo'lishi kerak;

e) tarmoq kabellari ulangan o'zaro faoliyat va kommutatsiya uskunalari himoyalangan xonalarga yoki yopiq kommutatsiya shkaflariga joylashtirilishi kerak;

f) foydalanilmayotgan tarmoq portlari telekommunikatsiya va server uskunalarini boshqarish vositalari orqali o'chirilishi kerak;

g) oraliq va oxirgi kabel yotqizish punktlarining xonalari va shkaflari qulflangan bo'lishi kerak;

h) ruxsat etilmagan qurilmalarni kabel tarmog'iga ulash uchun tekshirishlar (zondlash yoki fizikaviy tekshirish) o'tkazilishi kerak.

154. Axborot tashqi telekommunikatsiya tarmoqlari va korporativ tarmoq orqali uzatilganda uning konfidensialligini ta’minlash maqsadida quyidagi himoya choralari ko‘riladi:

a) Bankning tarkibiy bo‘linmalarini tashqi axborot tizimlari ulashda va bank xodimlarining axborot tizimlariga kirishini ta’minlashda korporativ tarmoqda, shuningdek bank axborot tizimlari bilan o‘zaro aloqada bo‘lganda tashqi tarmoqda xavfsiz tarmoq ulanishlarini tashkil etish va ulardan foydalanish;

b) uchinchi shaxslar bilan xabar almashish (xat yozishmalar) uchun E-xat xavfsiz axborot uzatish tizimidan foydalanish.

155. Korporativ tarmoqda xavfsizlikni tashkil etishga qo'yiladigan talablar siyosatning 1-ilovasiga muvofiq korporativ va himoyalangan tarmoqlarni ulanishlarini tashkil etish bo’yicha nizom asosida amalga oshiriladi.

156. Bank korporativ tarmog‘ida xavfsiz tarmoq ulanishlari sifatida VPN ulanishlari IPSec protokoli yordamida, shuningdek https, SSL/TLS, SSH protokollaridan foydalangan holda xavfsiz ulanishlardan foydalaniladi. Ushbu xavfsiz ulanishlarning tavsifi va parametrlari siyosatning 1-ilovasiga muvofiq korporativ tarmoq va xavfsiz tarmoq ulanishlarini tashkil etish to'g'risidagi nizomda keltirilgan.

157. Bankning ichki axborot tizimlari, resurslari va uskunalariga tashqi tarmoq orqali masofadan kirishni tashkil etish cheklanishi kerak. Agar kerak bo'lsa, ushbu masofaviy kirishni tashkil qilishda xavfsiz VPN ulanishlaridan foydalanadi.

158. Bank korporativ tarmoqni tashqi internet tarmog‘iga ulash chegarasida tashkil etilgan bankning yagona proksi-serveri orqali bank xodimlari uchun Internet tarmog‘iga kirishni ta’minlaydi.

159. Bankda lokal tarmoqlarni qurishda shuningdek, bank korporativ

tarmog‘iga kirish nuqtalarini tashkil qilishda Wi-Fi texnologiyalaridan foydalanish cheklanishi kerak.

160. Bankda simsiz Wi-Fi tarmog‘i mijozlarni jalb qilish va ularga qulaylik yaratish – Bankka tashrif buyurganlarida internetdan bepul foydalanishni ta’minlash maqsadida faqat AB, MBXO ва BXM old zonalarida tashkil etilgan.

Mazkur Wi-Fi tarmog‘i bank tomonidan mahalliy tarmoqlar va bank korporativ tarmog‘i bilan jismoniy aloqaga ega bo‘lmagan, Internet tarmog‘iga markazlashtirilgan holda kirish imkoniyatiga ega bankda alohida umumiy tarmoq shaklida tashkil etilgan.

XI. Javobgarlik taqsimoti

161. Axborot xavfsizligi rejimini yaratish va qo‘llab-quvvatlash uchun bank va uning alohida resurslari axborot xavfsizligini ta’minlash, shuningdek, uzluksiz ishlashini ta’minlash va uning faoliyatini tiklash kabi ma’lumotlarni himoya qilishning muayyan tartib-qoidalarini amalga oshirish uchun javobgarlikni aniq hujjatlashtirish zarur.

162. Resurslarni taqsimlash va axborot xavfsizligini ta’minlash tartib-taomillarini amalga oshirish uchun javobgarlik bank rahbariyati hamda Bosh ofis, AB, MBXO ва BXM tuzilmaviy bo‘linmalari rahbarlari zimmasiga yuklanadi.

163. Bank rahbariyatining axborot xavfsizligini ta’minlash bo‘yicha asosiy vazifalari quyidagilardan iborat:

1) Bank talablariga javob beradigan axborot xavfsizligini ta’minlashning maqsad va tamoyillarini belgilash;

2) Bank axborot xavfsizligini boshqarishning tashkiliy tuzilmasini belgilash va o‘zgartirish;

3) vazifalarni taqsimlash va axborot xavfsizligi uchun mas'ul shaxslarni tayinlash;

4) Bankning axborot xavfsizligini ta’minlash uchun zarur bo‘lgan resurslarini taqsimlash yoki ajratish;

5) Bank tarkibiy bo‘linmalari va xodimlarining axborot xavfsizligini ta’minlash sohasidagi tashabbuslarini muvofiqlashtirish va qo‘llab-quvvatlash;

6) Bank doirasida axborot xavfsizligini ta’minlash sohasidagi loyihalarni tasdiqlash;

7) Bankning barcha loyihalariga axborot xavfsizligi talablarini kiritishni hisobga olish;

8) Bankning yangi tizimlari yoki xizmatlari uchun axborot xavfsizligini boshqarish bo‘yicha aniq chora-tadbirlarning muvofiqligini baholash va amalga oshirilishini muvofiqlashtirish;

9) axborot xavfsizligini hodisalarini tekshirish natijalarini tahlil qilish, aybdorlarni javobgarlikka tortish;

10) xodimlarni qo'llab-quvvatlash rag'batlantirish, axborot xavfsizligini ta'minlash samaradorligiga erishishga hissa qo'shish va boshqalar.

164. Bankda AXBTni bevosita tashkil etish va samarali faoliyat ko‘rsatilishi Xavfsizlik va axborotlarni muhofaza qilish departamenti va uning bo‘linmalariga yuklatilgan bo‘lib, ularning vazifalari va majburiyatlari siyosatga 4-ilovasida belgilangan.

165. Axborot texnologiyalari departamenti Bank axborot xavfsizligini ta’minlash, axborotlashtirish vositalariga texnik xizmat ko‘rsatish va ulardan foydalanish jarayonlarida ham ishtirok etadi.

166. Bank va uning tarkibiy bo‘linmalari buyrug‘i bilan Axborot texnologiyalari departamenti xodimlari orasidan axborotlashtirish obyektlariga texnik xizmat ko‘rsatish va ularning uzluksiz ishlashini ta’minlash uchun mas’ul xodimlar (keyingi o‘rinlarda - administratorlar) tayinlanadi.

167. Mazkur siyosat Bankda axborot xavfsizligini ta’minlash bo‘yicha quyidagi javobgarlikni taqsimlashni belgilaydi:

1) Bankda axborot xavfsizligini ta’minlash bo‘yicha barcha tadbirlar uchun Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori javobgardir;

2) Xavfsizlik va axborotlarni muhofaza qilish departamenti Axborotlarni muhofaza qilish boshqarmasi boshlig‘i bankda axborot himoyasi va axborotlashtirish obyektlarini himoya qilish nuqtai nazaridan axborot xavfsizligini ta’minlash uchun javobgardir;

3) Xavfsizlik va axborotlarni muhofaza qilish departamenti bank xavfsizligi boshqarmasi boshlig‘i Bankda xonalari va moddiy boyliklarning jismoniy muhofazasini ta’minlash uchun javobgardir;

4) MBXOdagi Xavfsizlik va axborotni muhofaza qilish bo’limi boshlig'i MBXO, BXM va ularga qarashli masofaviy kassalardagi xonalar va moddiy boyliklarning axborot xavfsizligi va jismoniy muhofazasini ta'minlash uchun javobgardir;

5) Bank axborotlashtirish vositalari va ularning obyektlarining uzluksiz ishlashini ta’minlash va faoliyatini tiklash uchun mas’ul shaxslar siyosatining 21-ilovasida ko‘rsatilgan;

6) Bank xodimlari, shuningdek axborot aktivlari egalari himoyalangan ma’lumotlarning (har qanday shaklda) konfidensialligini buzganlik uchun shaxsan javobgar bo‘ladilar;

7) Bank axborot tizimlarida amalga oshirilayotgan harakatlar uchun Bankning axborot tizimlaridan foydalanuvchilari bo‘lgan xodimlari o‘zlariga yuklangan rol va majburiyatlar doirasida javobgar bo‘ladilar;

8) ish stansiyasining, mobil va boshqa qurilmalar axborot tashuvchilarning axborot xavfsizligi (jumladan, jismoniy xavfsizligi) uchun xizmat vazifalarini bajarish uchun ushbu qurilmalar yoki axborot tashuvchilar taqdim etilgan bank xodimi javobgar bo'ladi;

9) yong'in va texnik xavfsizlik, har bir bino ichidagi asbob-uskunalarning xavfsizligini ta'minlash uchun bank bosh ofis, AB, MBXO ва BXMning tarkibiy bo'linmalari rahbarlari, shuningdek bankning Xavfsizlik va axborotlarni muhofaza qilish departamenti bank xavfsizligi boshqarmasi boshlig'i mas'uldir.

168. Xavfsizlik va axborotlarni muhofaza qilish departamenti, shuningdek Axborot texnologiyalari departamenti o‘z tarkibiy bo‘linmalarining axborotni qayta ishlash, saqlash, uzatishning muayyan vositalari va axborotni himoya qilish vositalarining ishlashi va ulardan foydalanish uchun mas’ul xodimlarini belgilaydi.

169. Ushbu bolimning 167-bandda ko‘rsatilgan javobgarlik xodimlarning lavozim yo‘riqnomalarida va bankning boshqa axborot xavfsizligiga tegishli bo‘lgan ichki me’yoriy hujjatlarda belgilanadi.

170. Mas'ul shaxs yo'q bo'lganda (ta'til, kasallik, xizmat safari va boshqalar tufayli) uning vazifalari belgilangan tartibda tayinlangan shaxs tomonidan amalga oshiriladi. Bu shaxs tegishli huquqlarga ega bo'ladi va o'ziga yuklangan vazifalarni to'g'ri bajarish uchun javobgardir.

171. Bankda vazifa va majburiyatlarni taqsimlash uchun:

a) Bank uskunalari va axborot xavfsizligi vositalari himoya qilinadigan obyektlarga, shu jumladan konfidensial ma'lumotlarga, ma'lumotlarni qayta ishlash markazlariga, server xonalariga va boshqa yuqori darajadagi xavfsizlik xonalariga (3-zona), lokal va korporativ tarmoqlarga, ABT va boshqa axborot tizimlari va resurslariga, tarmoqqa jismoniy va mantiqiy kirish huquqiga ega bo'lgan shaxslar ro'yxati belgilanadi;

b) mobil qurilmalari, ma'lumotlarni saqlaydigan hamda tashuvchi disklari bank xodimlariga tashkiliy-ma'muriy hujjatlar bilan biriktiriladi;

c) Bank Xavfsizlik va axborotlarni muhofaza qilish departamenti va Axborot texnologiyalari departamenti boshliqlari, bank axborot xavfsizligini ta'minlashga mas'ul shaxslar bo'yicha o'zlariga yuklangan vazifalarning bajarilishi ustidan nazoratni amalga oshiradi.

XII. Siyosatni qayta ko'rib chiqish va yangilash tartibi

172. Xavfsizlik va axborotlarni muhofaza qilish departamenti o'zining tarkibiy bo'linmalari bilan birgalikda bank Axborot xavfsizligi siyosati qoidalari va talablarining dolzarbligi va:

bank siyosatining amaldagi tashkiliy-texnologik va axborot infratuzilmasiga hamda ularni bankda yanada rivojlantirish istiqbollariga muvofiqligi;

siyosatining amaldagi me'yoriy hujjatlar talablariga muvofiqligi;

siyosatda belgilangan talablarning muvofiqligi va yetarliligi;

siyosatda belgilangan usul va vositalarning samaradorligini baholaydi.

173. Siyosatning dolzarbligi va samaradorligini baholash yiliga kamida bir marta davriy ravishda Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan amalga oshiriladi.

174. Siyosatning dolzarbligi va samaradorligini baholash bank axborot infratuzilmasining tasdiqlangan siyosat talablari va qoidalariga muvofiqligi yuzasidan ichki yoki tashqi audit o'tkazish yo'li bilan amalga oshirilishi mumkin.

Axborot xavfsizligining ichki auditi bank Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan o'z mutaxassislarini jalb qilgan holda tashkil etiladi va amalga oshiriladi. Axborot xavfsizligining tashqi auditini o'tkazish uchun bunday auditni o'tkazishga vakolatli uchinchi tomon tashkilotlari jalb qilinadi.

175. Siyosatning dolzarbligi va samaradorligini baholash natijalariga ko'ra uni amalga oshirish jarayonida siyosatga o'zgartirish va qo'shimchalar kiritish yoki qayta ko'rib chiqish bo'yicha takliflar kiritilishi mumkin.

Mazkur siyosatga o'zgartirish va qo'shimchalar kiritish yoki qayta ko'rib chiqish bo'yicha takliflar Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan tayyorlanadi va bank rahbariyatiga kiritiladi.

Siyosatga o'zgartirish va qo'shimchalar kiritish yoki uni qayta ko'rib chiqish to'g'risidagi qaror bank boshqaruvi va kuzatuv kengashi tomonidan qabul qilinadi.

176. Siyosatga o'zgartirish va qo'shimchalar kiritish yoki qayta ko'rib chiqish bo'yicha takliflar quyidagi hollarda tuzilishi kerak:

siyosat qoidalari va talablari hamda bankdagi tashkiliy, texnologik va axborot infratuzilmasi o‘rtasidagi nomuvofiqliklar aniqlanganda;

siyosatning ayrim qoidalari va talablari, yangi yoki o‘zgartirilgan qonun hujjatlari va boshqa normativ-huquqiy hujjatlarga zid kelganda;

siyosatda belgilangan talablar, usullar va vositalarning yetarli emasligi yoki samarasizligini aniqlanganda.

bankning axborot xavfsizligi siyosatini takomillashtirish va bankda axborot xavfsizligini boshqarishga yondashuvlarni takomillashtirish zarurligini belgilash;

bankni qayta tashkil etish yoki qayta qurish;

bank AXBT tuzilmasi va tarkibidagi o‘zgarishlar;

bank axborot - kommunikatsiya infratuzilmasini rekonstruksiya qilish va modernizatsiya qilish;

biznes va texnologik jarayonlardagi o'zgarishlar va boshqalar.

177. Siyosatga o‘zgartirish va qo‘shimchalar kiritish yoki qayta ko‘rib chiqish quyidagi hollarda amalga oshiriladi:

bankning axborot xavfsizligi va uning jarayonlarini boshqarishga yondashuvini takomillashtirish;

nazorat, boshqaruv va axborot xavfsizligini ta’minlash chora-tadbirlari va vositalarini hamda ularni qo‘llash maqsadlarini takomillashtirish;

resurslarni va/yoki majburiyatni taqsimlashni takomillashtirish va javobgarlikni oshirish;

bank uchun axborot xavfsizligi tahdidlarini kamaytirish.

178. Agar siyosatni ayrim bandlari va boshqa me’yoriy hujjatlari, O’zbekiston Respublikasini axborot xavfsizligi sohasiga doir yangi qonuniy hujjatlariga zid bo‘lsa, bu holda siyosatga o‘zgartirish kiritilguniga qadar ushbu bandlar o‘z yuridik kuchini yo’qotadi.

179. Siyosatga o‘zgartirish va qo‘shimchalar bank boshqaruvi va kuzatuv kengashi qarori bilan kiritiladi.

180. Siyosat mazmunining 30% dan ortig‘ini o‘zgartirishga olib keladigan jiddiy o‘zgarishlar yuz bergan taqdirda, ushbu siyosat qayta ko‘rib chiqiladi.

Bank axborot xavfsizligi siyosatini qayta ko‘rib chiqilgandan so’ng uning yangi tahriri ishlab chiqilishi kerak.

181. Siyosatining yangi tahriri O’zbekiston Respublikasining Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi hamda O’zbekiston Respublikasi Davlat xavfsizlik xizmati bilan qayta kelishilishi shart.

182. Kelishuvdan so‘ng siyosatning yangi tahriri bank kuzatuv kengashi tomonidan tasdiqlanadi va bankning manfaatdor xodimlari va boshqa shaxslariga yetkaziladi.

183. Bank xodimlari, axborot xavfsizligi siyosati tasdiqlangandan keyin yoki qayta ko‘rib chiqilgandan keyin, Axborot xavfsizligi siyosatining 19-ilovasida shakli keltirilgan “Axborot xavfsizligi siyosati bilan tanishish jurnali”ni imzolash orqali tanishib chiqishlari shart.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
1-ilova

Korporativ va himoyalangan tarmoqlarni ulanishlarini tashkil etish bo‘yicha NIZOM

I. Umumiy qoidalar

1. Ushbu nizom “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – bank)ning korporativ tarmog‘i va himoyalangan tarmoq ulanishlarini tashkil etish hamda undagi axborot xavfsizligini ta’minlash qoidalari va tartiblarini belgilaydi.

2. Bank korporativ tarmog‘i O‘zbekiston Respublikasi Markaziy bankining bank telekommunikatsiya tarmog‘i (keyingi o‘rinlarda – BTT) va “O‘zbektelekom” AK ma’lumotlar uzatish tarmog‘ini ijaraga olingan kanallar yordamida qurilgan.

3. Asosiy ma’lumotlarni qayta ishlash markazi (keyingi o‘rinlarda MQIM deb yuritiladi), AB va zaxira ma’lumotlarni qayta ishlash markaziga ega bosh ofis (bitta binoda), bank xizmatlari ko‘rsatish markazlari (keyingi o‘rinlarda HXKM deb yuritiladi), bank xizmatlari markazlari (keyingi o‘rinlarda - BXKM deb yuritiladi), ochiq masofaviy tashkil etilgan universal bank kassalari (keyingi o‘rinlarda masofaviy kassalar deb yuritiladi).

4. Bank korporativ tarmog‘iga faqat ruxsat berilgan qurilmalar (ish stansiyalari, serverlar, bankomatlar) ulanishi kerak.

5. Bank tuzilmaviy tashkilotlari va axborotlashtirish obyektlarini korporativ tarmoqqa ulash to‘g‘risidagi qaror bank rahbariyati tomonidan qabul qilinadi va Axborot texnologiyalari departamentining Telekommunikatsiyalar va aloqa bo’limi va Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoya qilish boshqarmasi bilan birgalikda ta’minlanadi. Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoya qilish boshqarmasi va Axborot texnologiyalari departamenti bilan birgalikda belgilanadigan korporativ tarmoqqa xavfsiz ulanish talablarini belgilaydi.

6. Bank xodimlarining korporativ tarmoqqa ulanishi ularning bank axborot tizimlari va resurslaridan foydalanishini ta’minlash maqsadida amalga oshiriladi.

Foydalanuvchilarni bankning axborot tizimlari va resurslariga ulash va ro‘yxatdan o‘tkazish, bank tizimidagi resurslaridan foydalanuvchilarga kirish huquqini berish, o‘zgartirish va tugatish tartibi to‘g‘risidagi yo‘riqnomaga muvofiq amalga oshiriladi.

7. Bankning avtomatlashtirilgan bank tizimiga (keyingi o‘rinlarda ABT deb yuritiladi) ulangan yoki foydalaniladigan ish stansiyalari va serverlariga tashqi internet tarmog‘iga kirishni tashkil etish taqiqlanadi.

8. Bank tomonidan yaratilgan korporativ tarmoq sxemasi, Markaziy bankning BTT, internet va boshqa tashqi tarmoqlarga ulanishi O‘zbekiston Respublikasi Markaziy banki bilan kelishilgan holda amalga oshiriladi.

9. Axborot texnologiyalari departamentining Telekommunikatsiyalar va aloqa bo’limi hamda Xavfsizlik va axborotlarni muhofaza qilish departamentining

axborotni himoya qilish boshqarmasi tomonidan korporativ tarmoqning ishlashi va xavfsizligi ustidan muntazam ravishda to‘liq foydalanish hamda nazorat va monitoringini olib boradi.

II. Atamalar, ta’riflari va qisqartmalari

10. Ushbu nizom da quyidagi atamalar va ularning ta’riflari qo‘llaniladi

1) **virtual xususiy tarmoq (VPN):** Bu Internet kabi xususiy yoki umumiy tarmoqdagi nuqtali aloqa. VPN mijozlari tunnel protokoli deb nomlangan maxsus TCP/IP protokollaridan foydalanadilar, bu ikki kompyuter o‘rtasida xavfsiz ma’lumotlar almashish, kanalini o‘rnatishni ta’minlaydi.

2) **korporativ tarmoq:** bankning (tashkilotning) mahalliy axborot kompyuter tarmoqlarini (firmalari, tashkilotlari, aksiyadorlik jamiyatlari va boshqalar) birlashtiruvchi axborot-hisoblash tarmog‘i;

3) **lokal hisoblash tarmog‘i:** Bitta bino yoki bitta korxona bilan cheklangan bitta lokal zonada qator hisoblash texnikasi qurilmalarini bog‘laydigan axborot-hisoblash tarmog‘i

11. Ushbu nizomda quyidagi qisqartmalardan foydalaniladi;

DMZ (Demilitarized Zone) - demilitarizatsiya zonasi;

VLAN (Virtual Local Area Network) - virtual lokal tarmoq;

WAF (Web Application Firewall) - web ilovalar uchun tarmoqlararo ekran;

III. Korporativ tarmoqning maqsadi

12. Bank korporativ tarmog‘i bank boshqaruv tizimining ajralmas qismi bo‘lib, bankning tarkibiy bo‘linmalari o‘rtasida tezkor axborot almashish hamda bank xodimlarining axborot tizimlari va resurslaridan foydalanishini ta’minlashga mo‘ljallangan.

13. Bank korporativ tarmog‘i quyidagilarni ta’minlaydi:

bank bosh ofis va AB, MBXO, BXM xodimlarini bank ABT tizimi va serverlari asosiy va/yoki zaxira ma’lumotlarni qayta ishlash markazida joylashgan boshqa axborot tizimlariga ulash;

bank bosh ofis va AB, MBXO, BXM, masofaviy kassalari, korporativ va banklararo elektron pochta, IP-telefoniya va videokonferensiya aloqa xizmatlarini tashkil etish;

bankning asosiy va zaxiraviy ma’lumotlarni qayta ishlash markazida o‘rnatilgan yagona proksi-server orqali tashkil etilgan, bosh ofis va AB, MBXO, BXM, xodimlari internet tarmog‘iga markazlashgan holda ulash;

korporativ tarmoqning Markaziy bankning BTTga xavfsiz ulanishini tashkil etish, shuningdek, ABT Bankning Markaziy bank axborot tizimlari shuningdek, uchinchi tomon tashkilotlari axborot tizimlari bilan o‘zaro aloqa o’rnatish uchun xavfsiz kanallarni tashkil etish;

bankning ABT va Way4 protsessing tizimining HUMO, UzCard, VISA, MasterCard, UnionPay, JSB xalqaro plastik kartochkalari va boshqalar tashkilotlar bilan xavfsiz kanallar yoki alohida xalqaro aloqalar o’rnatish;

internet-banking va mobil banking interaktiv bank xizmatlarini ko'rsatish uchun bank mijozlarini Internet-banking va mobil banking tashqi web-ilovalari orqali ABT ga ulash;

bank SWIFT serverlarini alohida xalqaro ma'lumotlarni uzatish kanali orqali xalqaro SWIFT tizimiga ulash;

pul o'tkazmalari operatorlari va serverlarini Internet orqali pul o'tkazmalari tizimlariga ulash.

IV. Korporativ tarmoq tarkibi

14. Bank korporativ tarmog'iga quyidagilar kiradi:

telekommunikatsiya operatorlaridan ijaraga olingan ma'lumotlar uzatish kanallari shuningdek, korporativ tarmoqni tashqi tarmoqqa ulash kanallari, xalqaro ma'lumotlarni uzatish kanallari va uchinchi tomon axborot tizimlari bilan o'zaro hamkorlik qilish uchun tashkil etilgan kanallar;

asosiy va zaxira ma'lumotlarni qayta ishlash markazlari o'rtasida tashkil etilgan shaxsiy OTAL;

korporativ tarmoq kommutator yadrosi;

asosiy ma'lumotlarni qayta ishlash markazining korporativ tarmog'iga ulanishni ta'minlaydigan tarmoq telekommunikatsiya uskunalari (marshrutizatorlar, modemlar), bosh ofis (AB va zaxira ma'lumotlarni qayta ishlash markazi), MBXO, BXM, bankning masofaviy kassalari va bankomatlari; shuningdek, korporativ tarmoqni tashqi tarmoqlarga va ma'lumotlarni uzatishning xalqaro kanallariga ulash;

bankning tarmoqlararo ekran, IDPS hujumlarini aniqlash va oldini olish vositalari, proksi-serverlar, VPN vositalari.

15. Bundan tashqari, bank korporativ tarmog'iga quyidagi xizmatlar va axborot almashish tizimlari kiradi:

1) Bank bosh ofis, AB, MBXO ва BXM xodimlari uchun korporativ elektron pochta;

2) Bank O'zbekiston Respublikasi Markaziy banki va respublikaning boshqa banklari o'rtasida axborot almashish uchun mo'ljallangan banklararo elektron pochta tizimi;

3) IP-telefoniya tizimi, shuningdek bank mijozlari bilan o'zaro hamkorlik qilish uchun Call-markaz (operatorlar ish o'rinlarini tashkil etish bilan aloqa markazi);

4) Bankning videokonferensaloqa tizimi;

5) Bosh ofisi va ijroni nazorat qilish departamenti va MBXO tarkibiy bo'linmalari devonxona bo'limlari xodimlari uchun tashkil etilgan E-xat xavfsiz elektron pochta manzili.

V. Korporativ tarmoq ishlash tamoyillari

16. Korporativ tarmoq hududiy jihatdan taqsimlangan axborot-telekommunikatsiya tarmog'idir.

17. Bank har bir MBXO va BXM “O‘zbektelekom” AK va Markaziy bankning BTT operatorlarining ikkita ijaraga olingan kanallari orqali bevosita asosiy ma’lumotlarni qayta ishlash markaziga ulangan.

18. Har bir masofaviy kassa ham Markaziy bankning BTT orqali ijaraga olingan bitta kanaldan foydalangan holda to'g'ridan-to'g'ri asosiy ma'lumotlarni qayta ishlash markaziga ulangan.

19. Bankning bank obyektlari ichida joylashgan bankomatlarini ulash korporativ tarmoq orqali Way4 protsessing tizimi va UzCard protsessing tizimiga, bank obyektlaridan tashqarida joylashgan Bankomatlar esa ularga ma’lumotlar uzatish simli ulanishi, tarmoq operatorlari yoki 3G uyali tarmoq va 4G yordamida ulanadi.

20. Asosiy ma'lumotlarni qayta ishlash markaziga, bosh ofis (AB va zaxira zaxira ma’lumotlarni qayta ishlash markazi), MBXO va BXMni korporativ tarmoqqa ulash uchun apparat va dasturiy marshrutizatorlardan foydalaniladi.

Masofaviy kassalar korporativ tarmoqqa ADSL modemlari yoki 3G/4G modemlari shuningdek, apparat va dasturiy mashurtizatorlar yordamida ulangan.

21. VPN tunnellari asosiy ma'lumotlarni qayta ishlash markazi va ularga ulangan bosh ofis (AB), MBXO, BXM, masofaviy kassalar o'rtasida ularning ulanish chegarasida marshrutizatorlar o'rnatilgan korporativ tarmoq yordamida tashkil etilgan.

22. Bank korporativ tarmog‘i tashqi tarmoqlarga quyidagi ulanishlarga ega:

1) OneNet telekommunikatsiya operatori orqali internetga:

bank xodimlariga va alohida serverlarga proksi-server orqali internet tarmog‘iga kirishni ta’minlash;

proksi-server orqali bankning operatorlari yoki pul o'tkazmalari serverlarini xalqaro va xorijiy pul o'tkazmalari tizimlariga ulash;

interaktiv bank xizmatlarini ko‘rsatish uchun tashqi internet foydalanuvchilari va bank mijozlarini internet-banking va mobil banking tashqi web-ilovalariga ulash;

tashqi foydalanuvchilar bilan pochta trafigini, IP-telefoniya trafigini almashishni ta'minlash.

2) O‘zbekiston Respublikasi Markaziy banki BTTga:

bankning Markaziy bankning bank tizimlari, shuningdek, boshqa tashqi axborot tizimlari bilan o‘zaro hamkorligi;

bankning ABT va Way4 protsessing tizimini UzCard va HUMO protsessing markazlariga ulash;

Markaziy bank bilan pochta trafigini almashish (Banklararo elektron pochta);

3) xalqaro ma'lumotlarni uzatish kanallarini quyidagilar uchun ajratish:

bankning Way4 protsessing tizimini xalqaro bank kartalari protsessing tizimlariga ulash;

Bank SWIFT serverini xalqaro SWIFT tizimiga ulash.

23. Bank mijozlari uchun AB, MBXO va BXM front zonalarida tashkil etilgan Wi-Fi tarmoqlari mahalliy tarmoqlarga va bankning korporativ tarmog‘iga jismoniy ulanishga ega emas va korporativ tarmoqdan alohida markazlashtirilgan internetdan foydalaniladi.

24. Bank korporativ tarmog‘ini internet va Markaziy bankning BTT tashqi tarmoqlariga, shuningdek, xalqaro aloqaning tashqi kanallariga ulanish tarmoqlararo ekran va IDPS vositalari orqali tashkil etiladi.

25. Internet-banking va mobil banking uchun ishlatiladigan web-ilovalarni himoya qilish, shuningdek, tashqi axborot tizimlari bilan o'zaro aloqa qilish uchun asosiy ma'lumotlarni qayta ishlash markazida joylashgan WAF web-ilovasining tarmoqlararo ekran ishlatiladi.

26. Korporativ tarmoq bank xodimlarining asosiy va zaxiraviy ma’lumotlarni qayta ishlash markazlarida proksi-server orqali internet tarmog‘iga markazlashgan holda kirishini ta’minlaydi. Mazkur xodimlar ro‘yxati bank rahbariyati tomonidan belgilanadi. Shu bilan birga, ushbu xodimlarga internetning ma'lum resurslariga (oq ro'yxati), xususan, xalqaro va xorijiy pul o'tkazmalari tizimlariga kirish imkoniyati ta'minlanadi.

27. Bankning ichki axborot tizimlarini internet tarmog‘iga to’g’ridan to’g’ri ulashga yo‘l qo‘yilmaydi. Shuningdek, bank xodimlari tomonidan ko‘rsatilgan ichki axborot tizimlariga tashqi internet tarmog‘i orqali masofadan kirishini tashkil etishga yo‘l qo‘yilmaydi.

28. Asosiy va zaxira ma'lumotlarni qayta ishlash markazi (bosh ofisda) o'rnatilgan ABT saqlash tizimlari ma'lumotlarini arxivlash uchun asosiy va zaxira ma'lumotlarni qayta ishlash markazlari o'rtasida alohida SAN kommutatorlari tashkil etilgan.

29. Korporativ tarmoq bazasida bankning yagona boshqariladigan domen tarmog‘i bosh ofis (AB) MBXO, BXM, masofaviy kassalar korporativ tarmog‘iga ulangan barcha obyektlar (ish stansiyalari, serverlari va boshqalar) uchun ichki IP-manzillardan foydalangan holda bitta domen ostida tashkil etilgan. Bankning yagona domen tarmog‘ini tashkil etish uchun asosiy va zaxira ma’lumotlarni qayta ishlash markazlarida mos ravishda o‘rnatilgan DNS domen serverlari (keyingi o‘rinlarda domen kontroller serverlari deb yuritiladi) qo‘llaniladi. Shuningdek Way4 bank plastik kartochkalarini qayta ishlash tizimi va unga ulangan tegishli tarkibiy bo‘linmalari uchun alohida domen kontroller serveri yordamida boshqariladigan domen tarmog‘i yaratiladi.

30. Korporativ tarmoq, tarmoq infratuzilmasiga hajmni optimallashtirish, axborot xavfsizligini ta'minlash, tarmoqning server segmentini tashqi ta'sirlardan cheklash maqsadida izolyatsiyalangan (VLAN) segmentlarga bo'lingan.

31. Izolyatsiya qilingan tarmoq segmentlarida (DMZ) asosiy va muhim axborot tizimlari (ABT va boshqa to'lov tizimlari, internet-banking, SWIFT, Way4 protsessing tizimi va boshqalar) serverlari mavjud.

32. DMZ asosiy ma'lumotlarni qayta ishlash markazining lokal tarmog'idan apparat va dasturiy tarmoqlararo ekran bilan ajratilgan.

VI. Korporativ tarmoqni tashkiliy boshqarish va rivojlantirish bo‘yicha ishlarni tashkil etish

33. Korporativ tarmoqni tashkiliy boshqarish va undan foydalanish, uni rivojlantirish yo‘nalishlari va bosqichlarini belgilash, shuningdek, uni rivojlantirish bo‘yicha chora-tadbirlarni amalga oshirish Axborot texnologiyalari

departamentining Telekommunikatsiya va aloqa bo‘limi, Xavfsizlik va axborotlarni muhofaza qilish departamentining axborot xavfsizligi boshqarmasi bilan kelishilgan holda amalga oshiriladi.

34. Axborot texnologiyalari departamentining Telekommunikatsiyalar va aloqa bo‘limi tomonidan korporativ tarmoq administratori tashkil etiladi. Buning uchun bank korporativ tarmog‘i administratori tayinlangan.

35. Korporativ tarmoq administratori o‘z xizmat vazifalarini bajarish uchun Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi, Active Directory tizimi administratori, ma’lumotlarni uzatish kanallarini ijaraga beruvchi va tashqi tarmoqlarga ulanishni ta’minlovchi telekommunikatsiya operatorlari bilan va zarur hollarda MBXOning axborot texnologiyalari bo'limlari bilan o‘zaro hamkorlik qiladi.

36. Korporativ tarmoqni boshqarish quyidagilarni o'z ichiga oladi:

xavfsiz tarmoq ulanishlarini tashkil etish;

korporativ tarmoqning tashqi telekommunikatsiya tarmoqlari bilan axborot almashinuvini (trafikni) boshqarish;

korporativ tarmoq ichidagi axborot oqimlarini (trafikni) boshqarish;

bank xodimlarining korporativ tarmoq orqali axborot resurslari va tizimlariga kirishini boshqarish, ularning vakolatlari va foydalanish huquqlarini belgilash;

bank xodimlarining, axborot tizimlari va resurslarining tashqi tarmoqlarga kirishini boshqarish;

bank tarkibiy bo‘linmalari va axborotlashtirish obyektlarini korporativ tarmoq va tashqi tarmoqlarga ulash va o‘chirish;

korporativ tarmoq tarkibiga kiruvchi tarmoq uskunalari, tarmoq resurslariga texnik xizmat ko'rsatish va ularning ishlashini ta'minlash;

korporativ tarmoqda foydalaniladigan dasturiy va texnik vositalarni tanlash.

37. Korporativ tarmoq administratori siyosatga 3-ilovada keltirilgan korporativ tarmoq administratori uchun yo‘riqnomaga muvofiq korporativ tarmoqning uzluksiz ishlashini ta’minlash choralarini ko‘radi.

38. Korporativ tarmoq administratori Telekommunikatsiyalar va aloqa bo’limi boshlig‘ini yoki Axborot texnologiyalari departamenti direktorini nosozlik va shunga o’xshash boshqa barcha holatlari to‘g‘risida xabardor qilishi shart.

Korporativ tarmoq administratori korporativ tarmoqdagi axborot xavfsizligi hodisalari to‘g‘risida Xavfsizlik va axborotlarni muhofaza qilish departamentini xabardor qilishi shart.

39. Internet proksi-serverlari, tarmoqlararo ekran, IDPS vositalari, tarmoqlararo ekran funksiyalariga ega marshrutizatorlar, VPN vositalari Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan yuritiladi.

40. Bank domen-kontroller serverlarini administratorligi Axborot texnologiyalari departamentining Telekommunikatsiyalar va aloqa bo‘limi, Active Directory tizim administratori tomonidan amalga oshiriladi.

41. Korporativ tarmoqni rivojlantirish bo‘yicha takliflar Axborot texnologiyalari departamentining tarkibiy bo‘linmalari tomonidan shakllantiriladi

va mazkur Departament direktori va Bank rahbariyatiga tasdiqlash uchun taqdim etadi.

42. Axborot texnologiyalari departamenti tomonidan korporativ tarmoqni rivojlantirish bo‘yicha chora-tadbirlar rejasi shakllantirilib, Xavfsizlik va axborotlarni muhofaza qilish departamenti bilan kelishiladi va bank rahbariyati tomonidan tasdiqlanadi. Korporativ tarmoqni rivojlantirish bo'yicha chora-tadbirlar rejasi zarur texnik hujjatlarni ishlab chiqish, zarur jihozlarni sotib olish, shartnomalar tuzish, uskunalarni etkazib berish va o'rnatish va boshqalarni ko'zda tutishi kerak.

VII. Korporativ tarmoqni rivojlantirish

43. Bank korporativ tarmog‘ini yanada rivojlantirishning asosiy yo‘nalishlari quyidagilardan iborat:

korporativ tarmoq va tashqi tarmoqlardan tarmoq yukini asosiy va zaxira ma’lumotlarni qayta ishlash markazlari o‘rtasida taqsimlanishini ta’minlash;

asosiy va zaxira ma’lumotlarni qayta ishlash markazlari o'rtasida tarmoq uskunalari sig'imini taqsimlash (issiq zaxirani ta'minlash);

individual tarmoqlararo ekran va boshqa tarmoq xavfsizligi vositalarini modernizatsiya qilish;

bank xodimlarining so‘nggi qurilmalarining MAC manzillari bo‘yicha autentifikatsiya qilish asosida bank axborot tizimlariga kirishni alohida tarmoqlararo ekranda filtrlash va boshqarish sozlamalarini ta’minlash.

VIII. Axborot xavfsizligini ta’minlash va korporativ tarmoqda xavfsiz ulanishni tashkil etish prinsiplari

44. Korporativ tarmoqning axborot xavfsizligini ta’minlash quyidagi maqsadlar uchun zarurdir:

axborot, tarmoq va dasturiy resurslariga ruxsatsiz kirish va zarar yetkazish harakatlaridan himoya qilish;

korporativ tarmoq orqali uzatiladigan ma’lumotlarning konfidensialligini ta’minlash;

tarmoqning ishlashi buzilgan taqdirda tarmoqning axborot resurslari xavfsiz saqlanishini ta’minlash;

axborot xavfsizligi sohasidagi me’yoriy hujjat talablarga muvofiqligini ta’minlash.

45. Korporativ tarmoqning axborot xavfsizligini ta'minlash:

siyosatga 2-ilovada keltirilgan tarmoq infratuzilmasi darajasida axborot xavfsizligini ta’minlash va tarmoq himoyasi to‘g‘risidagi nizom talablariga muvofiq tarmoq xavfsizligini ta’minlashning boshqa vositalaridan va tarmoq xavfsizligini ta’minlashning boshqa vositalaridan foydalanish;

korporativ tarmoqni tashqi tarmoqqa, shu jumladan Internet, Markaziy bank BTS va boshqa tashqi ma’lumotlarni uzatish kanallariga ulashda, tarmoq bosqinlari va tashqaridan hujumlardan himoya qilish uchun IDPS hujumlarini aniqlash va oldini olish vositalaridan foydalanish;

asosiy va zaxira ma'lumotlar markazlarining maxsus xonalarida ruxsatsiz foydalanuvchilar kirishini cheklash, RCB va CBU kommutatsiya xonalarida axborotni qayta ishlash va saqlash vositalarini, tarmoq uskunalarini va axborotni himoya qilish vositalarini joylashtirish;

siyosatga 8-ilovada keltirilgan virusga qarshi himoya qilish bo‘yicha yo‘riqnomada ko‘rsatilgan chora-tadbirlar orqali korporativ tarmoqni zararli dasturlarning tarqalishidan himoya qilishni tashkil etish;

ruxsat etilmagan shaxslarning korporativ tarmog‘iga ruxsatsiz mantiqiy ulanishini hamda ulardan foydalanishni nazorat qilish va cheklash bo‘yicha chora-tadbirlarni amalga oshirish orqali korporativ tarmoq orqali axborot resurslari va tizimlariga kirishini istisno qilish;

bank korporativ tarmog‘ida ushbu nizomning 10-bo‘limiga muvofiq xavfsiz ulanishni tashkil etish.

46. Korporativ tarmoqning axborot xavfsizligini va unga kiritilgan axborotni himoya qilish vositalarining ishlashini ta'minlash bo'yicha chora-tadbirlar Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan amalga oshiriladi.

IX. Himoyalangan ulanish tasnifi

47. Bankda korporativ tarmoqdagi himoyalangan ulanishlar telekommunikatsiya tarmog‘i orqali uzatiladigan ma’lumotlarning konfidensialligi va yaxlitligini ta’minlash uchun ishlatiladi.

48. Bankning korporativ tarmoqdagi xavfsiz ulanishlar ikkita mezon bo‘yicha tasniflanadi:

ularni tashkil etish darajasi;

himoya qilishning amaliy texnologiyalari.

49. Bank korporativ tarmog‘idagi xavfsiz ulanishlar tashkiliy darajasi bo‘yicha quyidagilar tasniflanadi:

1) Bosh ofis (AB), MBXO, BXM, masofaviy kassalar o'rtasida aloqa va axborot almashinuvini tashkil qilish uchun xavfsiz ulanishlar (bankning tarkibiy bo'linmalari o'rtasida ma'lumotlar almashinuvi) bo’yicha.

2) Bank ABT va boshqa axborot tizimlarining Markaziy bankning bank axborot tizimlari, UzCard, HUMO protsessing tizimlari, xalqaro plastik kartochkalari va uchinchi tomon tashkilotlarining boshqa tashqi axborot tizimlari bilan o‘zaro aloqasi davomida xavfsiz ulanishlarni ta’minlash. (Bankning axborot tizimlari va uchinchi tomon axborot tizimlari o'rtasida ma'lumotlar almashinuvi).

3) Bank internet-banking va mobil banking web-resurslariga, bank rasmiy web-saytiga (bank mijozlari va axborot tizimlari, bank resurslari o‘rtasida ma’lumotlar almashinuvi) bank mijozlarining internet tarmog‘i orqali kirishini uchun xavfsiz ulanishlarni ta’minlash.

4) Bank ma’lumotlarni qayta ishlash markazida administratorlarning o‘z ish stansiyalaridan tarmoq va server uskunalariga masofaviy ulanishi uchun xavfsiz ulanishlar, bank ma’lumotlarni qayta ishlash markazida korporativ tarmoq va lokal tarmoqlar orqali (administratorlar va servis uskunalari o‘rtasida ma’lumotlar almashinuvi).

50. Qo'llaniladigan himoya texnologiyalari ko'ra, bank korporativ tarmog'idagi himoyalangan ulanishlar quyidagicha tasniflanadi:

1) VPN texnologiyalar yordamida himoyalangan ulanishlar;

2) HTTPS, SSL/TLS protokollar yordamida himoyalangan ulanishlar;

3) SSH tarmoq protokoli yordamida himoyalangan ulanishlar.

X. Korporativ tarmoqda himoyalangan ulanishlarni tashkil etish va ulardan foydalanish tamoyillari

51. Bank korporativ tarmog‘ida quyidagi xavfsiz ulanishlar tashkil etilgan:

a) asosiy ma'lumotlarni qayta ishlash markazi va unga ulangan Bosh ofis (AB), MBXO, BXM, masofaviy kassalar o'rtasida marshrutizatorlardan foydalangan holda VPN tunnellarini tashkil qilish bilan korporativ tarmoqdagi xavfsiz ulanishlarni ta'minlash. ushbu obyektlarni korporativ tarmoqqa ulash chegarasida o'rnatilgan VPN funksiyasi.

Ushbu xavfsiz ulanishlar VPN GRE texnologiyalari va IPSec protokoli yordamida tashkil etilgan.

Ushbu xavfsiz ulanishlar asosiy ma'lumotlarni qayta ishlash markazi va bank obyektlari o'rtasida korporativ tarmoqda xavfsiz ma'lumot almashish uchun tashkil etiladi va foydalaniladi.

Korporativ tarmoqdagi ushbu xavfsiz ulanishlar Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan ta'minlanadi.

b) Markaziy bankning axborot tizimlariga, bank va xalqaro plastik kartochkalarni qayta ishlash tizimlariga, xalqaro SWIFT tizimiga va boshqa uchinchi tomon axborot tizimlariga Markaziy bankning BTT, xalqaro aloqa kanallari yoki internet orqali ulanish.

Bank axborot tizimlari va uchinchi tomon tashkilotlarining axborot tizimlari o‘rtasida xavfsiz axborot almashinuvi VPN texnologiyalaridan va IPSec protokolidan foydalangan holda tashkil etiladi.

Ushbu xavfsiz ulanishlar Xavfsizlik va axborotlarni muhofaza qilsih departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan Markaziy bank, qayta ishlash tizimlari operatorlari va boshqa uchinchi tomon axborot tizimlari bilan hamkorlikda amalga oshiriladi.

c) Bank web-resurslariga internet-banking web-ilovasi va rasmiy web-saytiga internet orqali tashqi foydalanuvchilarga (bank mijozlariga) kirishni ta’minlashda https, SSL/TLS protokollaridan foydalangan holda xavfsiz https ulanishlaridan foydalanish, shuningdek, mobil banking tizimining web-ilovasi bilan mobil ilovalari o‘rtasida ma’lumot almashishda TLS protokolidan foydalangan holda xavfsiz ulanish tashkil etiladi.

Ularning tashkil etilishiga Axborot texnologiyalari departamentining Raqamli texnologiyalar va masofaviy bank tizimlarini qo‘llab-quvvatlash bo‘limi mas’uldir.

d) Bank ma’lumotlar markazida joylashgan tarmoq va server uskunalariga korporativ tarmoq va lokal tarmoqlar orqali administratorlar o‘z ish stansiyalaridan masofadan ulashda xavfsiz VPN ulanishlari va SSH ulanishlaridan foydalanish.

Masofaviy ulanish uchun ma'lumotlar markazida VPN shlyuzi administratorning ish stansiyalarida VPN texnologiyasi orqali ulanishlarini tashkil qilish uchun ishlatiladi va shifrlangan kanal va raqamli imzo autentifikatsiyasini ta'minlaydigan SSH tarmoq protokoli qo'llaniladi.

52. Yuqoridagi bandda ko'rsatilgan xavfsiz ulanishlarni tashkil etishni nazorat qilish Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi zimmasiga yuklanadi.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
2-ilova

Tarmoqlararo ekran va tarmoq infratuzilmasi darajasida axborot xavfsizligini ta’minlash to’g’risidagi NIZOM

I. Umumiy qoidalar

1. Ushbu nizom “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank) korporativ tarmog‘iga, tarmoqlararo ekrandan foydalangan holda axborot resurslari va tizimlariga kirishni boshqarish orqali axborot xavfsizligini ta’minlash mexanizmi va qoidalarini tartibga solish maqsadida ishlab chiqilgan.

2. Tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta’minlash to‘g‘risidagi nizom bank markaziy apparati va hududiy filiallarini axborot tizimlari va resurslarini tarmoq darajasida ruxsatsiz kirishdan himoya qilishni tashkil etishning asosiy tamoyillarini belgilaydi.

II. Atamalar va ta’riflar, qisqartmalar

3 Ushbu nizomda O’zDSt 2927:2015 va O’zDSt 1047:2018 davlat standartlaridagi atamalar va ularning ta’riflari qo‘llaniladi:

1) **tashqi tarmoq –** bank tomonidan nazorat qilinmaydigan tarmoqlar, shu jumladan Internet tarmog‘i, bankning Markaziy bank telekommunikatsiya tarmog‘i va boshqalar;

2) **DMZ zonasi** - (Demilitarized Zone) - demilitarizatsiya qilingan zona - axborot perimetrining muhofaza qilinishini ta'minlash texnologiyasi, bunda tashqi tarmoqdan kelayotgan so'rovlarga javob beruvchi yoki u erga so'rovlarni yuboruvchi serverlar tarmoqning alohida segmentida joylashgan;

3) **OSI modelining kanal (ikkinchi) darajasi** - kommutatsiya darajasida fizik manzilga murojaat qilish;

4) **tarmoqlararo ekran** – Tizimga kelib tushadigan va/yoki tizimdan chiqib ketadigan axborotning nazorat qilinishini amalga oshiradigan lokal (bir komponentli) yoki funksional taqsimlangan dasturiy (dasturiy-apparat) vosita (kompleks);

5) **OSI modeli** - Ochiq tizimlarning o’zaro bog’liqlik modeli. Xalqaro standartlashtirish tashkiloti tomonidan taklif qilingan ochiq tizimlarning yetti pog’onali o’zaro bog’lanish modeli;

6) **tarmoq infratuzilmasi -** bank korporativ tarmog‘ining aloqa liniyalarini, shuningdek ish stansiyalari va serverlar o‘rtasida mantiqiy aloqani ta’minlovchi kommutatsiya qurilmalarini o‘z ichiga olgan qismi;

7) **OSI modelining tarmoq (uchinchi) darajasi** - marshrutni va mantiqiy adresni IP protokoli darajasida aniqlash;

8) **OSI modelining fizik (birinchi) darajasi** - ma'lumotlarni uzatish vositasi, signallar va ikkilik ma'lumotlar bilan ishlash.

4. Mazkur nizom da quyidagi atamalar va ta'riflar ishlatilgan:
DMZ (Demilitarized Zone)– demilitarizatsiya zonasi;
VLAN (Virtual Local Area Network) — virtual lokal tarmoq;
WAF (Web Application Firewall) – web ilovalar uchun tarmoqlararo ekran.

III. Umumiy talablar va tarmoq infratuzilmasi darajasidagi talablar.

5. Tarmoq infratuzilmasini muhofaza qilish OSI modelining har bir sathini - jismoniy, kanal, tarmoq, transport va boshqalarni himoya qilishga asoslangan.

6. Jismoniy himoya qilish Bankda ma'lumotlarni uzatishda foydalaniladigan oddiy juftlik va optik kabellarining xavfsizligini ta'minlashdan iborat.

7. Bankda kanal sathidagi himoya tegishli axborot xavfsizligi funksiyalariga ega kommutatorlarga asoslangan holda qurilgan.

kirish ro'yxatini taqdim etish ACL (IP, MAC, VLAN);
portga kirishni cheklash (Port Security);
manzilni buzish funksiyalari (DHCP snooping, Dynamic ARP inspection, IP source guard);
eshittirish bo'ronlariga qarshi kurash mexanizmi (Storm Control);
boshqaruv darajasini himoya qilish (Control Plane Policing).

8. Tarmoqning uchinch bosqichi tarmoqlararo ekranlash modullari orqali himoya qilinadi.

9. Tarmoqlararo ekran belgilangan tarmoq xavfsizligi qoidalariga muvofiq ma'lumotlarni (paketlar va ulanishlarni) OSI modelining turli qatlamlarida (tarmoq sathidan ilova sathigacha) filtrlashi, shuningdek manzillarini yashirishi (IP-manzil translyatsiyasi) va tashqi foydalanuvchilar uchun himoyalangan tarmoq tuzilishi to'g'risidagi ma'lumotlarni yashirishi lozim..

10. OSIning 2 va undan yuqori sathlarini tarmoq hujumlardan himoya qilish hujumlarni aniqlash va oldini olish vositalari (IDPS) yordamida ta'minlanishi lozim.

IDPS vositasi tekshirish usuli va xatti-harakatlarni tahlil qilish usuli yordamida tarmoq hujumlari va hujumlarini aniqlashi va ularning harakatlarini oldini olish ta'minlanadi.

11. Bank tarmoqlararo ekran va IDPS vositalari sifatida tarmoqlararo ekran funksiyalarini amalga oshiruvchi yangi avlod NGFW apparat-dasturiy, tarmoqlararo ekran funksiyali marshrutizator va apparat-dasturiy tarmoqlararo ekran, IDPS hujumlarini aniqlash va oldini olish, ilovalar monitoringi va nazorati (AVC), zararli dasturlardan himoya qilish (Antivirus) va URL filtri. Yangi avlod NGFW tarmoqlararo ekran tomonidan hal qilinadigan tarmoq xavfsizligi vazifalari kompleksini hisobga olgan holda, ular bank himoyalangan korporativ tarmog'i uchun xavfsizlik shlyuzini tashkil etadi.

12. Internet-banking va mobil banking uchun ishlatiladigan web-ilovalarni himoya qilish, shuningdek, tashqi axborot tizimlari bilan o'zaro aloqa qilish uchun WAF web-ilovasining tarmoqlararo ekran qo'llaniladi.

IV. Tarmoqlararo ekrandan foydalangan holda axborot xavfsizligini ta'minlash uchun umumiy talablar

13. Bankda joriy qilingan tarmoqlararo ekran quyidagilarga ega bo'lishi kerak:

himoyalangan tarmoq yoki uning segmenti xavfsizligini ta'minlash va tashqi ulanishlar va aloqa seanslarini to'liq nazorat qilish;

siyosatni to‘liq va sodda tarzda amalga oshirish uchun kuchli va moslashuvchan boshqaruv vositalariga ega bo‘lish;

tarmoq strukturasini o'zgartirishda tizimni oddiy qayta konfiguratsiya qilishni ta'minlash;

tarmoq foydalanuvchilariga ko'rinmas holda ishlash va ularning qonuniy harakatlariga to'sqinlik qilmaslik;

barcha kiruvchi va chiquvchi trafikni "cho'qqi" rejimlarida qayta ishlash uchun yetarlicha samarali va o'z vaqtida ishlash (rivojlanishni hisobga olgan holda kerakli o'tkazish qobiliyatiga ega bo'lish);

har qanday ruxsatsiz ta'sirlardan o'zini himoya qilish xususiyatlariga ega bo'lish;

hodisalarni qayd etish va xavfsizlik bilan bog‘liq barcha harakatlarni qayd etish.

14. Tarmoqlararo ekran ulanish quyidagi chegarada o'rnatiladi:

bank korporativ tarmog‘i Internet tarmog‘iga;

bank korporativ tarmog‘i Markaziy bankning BTTga;

bank korporativ tarmog‘ini alohida tashqi aloqa kanallariga;

bosh ofisning lokal tarmog'i (AB va zaxira ma'lumotlarni qayta ishlash markazi) va korporativ tarmoqqa asosiy ma'lumotlarni qayta ishlash markaziga;

bank MBXO va BXM lokal tarmoqlari korporativ tarmoqqa;

asosiy ma'lumotlarni qayta ishlash markazining DMZ zonalari (ABT va boshqa to'lov tizimlari, SWIFT, Way4 ishlov berish tizimi va boshqalar) asosiy ma'lumotlarni qayta ishlash markazining lokal tarmog'iga va korporativ tarmoqqa.

15. 14-bandda ko‘rsatilgan tarmoqlararo ekran O‘z DSt 2815:2014 “Axborot texnologiyalari. Tarmoqlararo ekranlar. Ma’lumotlarga ruxsatsiz kirishdan himoya qilish darajasi bo‘yicha tasniflash” davlat standartiga muvofiq kamida 3 xavfsizlik sinfidan iborat bo‘lishi kerak.

16. Korporativ tarmoq tashqi tarmoqdan (Internet, Markaziy bankning BTT, xalqaro tizimlarga ulanish uchun xalqaro kanallar) apparat va dasturiy ta’minot tarmoqlararo ekrandan foydalangan holda himoyalangan bo‘lishi kerak, bu esa uni sozlashda quyidagi talablar bajarilishini ta’minlashi kerak:

tashqi tarmoqdan korporativ tarmoqqa kirishni bloklash, bundan interaktiv bank xizmatlarini ko‘rsatish uchun internet-banking va mobil banking mijozlari, shuningdek tashqi foydalanuvchilar bilan almashiladigan pochta va IP telefoniya trafigi bundan mustasno;

tashqi tarmoqqa faqat bank xodimlarining bunday kirishga ruxsati bo‘lgan ishchi stansiyalari va axborot tizimlariga kirishni ta’minlash, shuningdek, ushbu kirishni boshqarish va faqat ayrim tashqi resurslarga (oq ro‘yxat) kirishni ta’minlash;

siyosat talablarini bajarish maqsadida tarmoq so‘rovlari va trafikni filtrlash qoidalariga muvofiq portlar, protokollar, IP manzillar, URL manzillar bo‘yicha filtrlash;

tarmoq manzillarini NAT orqali namoyish qilish.

17. DMZ zonalarini asosiy ma'lumotlarni qayta ishlash markazining lokal tarmog'idan va bank korporativ tarmog'idan chegaralash uchun tarmoq trafigini va so'rovlarni filtrlash, shuningdek, ABT va boshqa axborot tizimlariga kirishni nazorat qilish uchun apparat-dasturiy tarmoqlararo ekrandan foydalanish kerak. Bank serverlari DMZ zonalarida joylashgan.

18. Asosiy ma'lumotlarni qayta ishlash markazining va bosh ofisning (AB va zaxira ma'lumotlarni qayta ishlash markazi) ulanish chegarasida, shuningdek, MBXO va BXMning korporativ tarmoqqa ulanish chegaralarida ruxsatsiz kirishni blokirovka qilish uchun apparat va dasturiy ta'minot tarmoqlararo ekrandan foydalanish kerak.

19. Amalga oshirishdan oldin tarmoqlararo ekran qoidalarning 6-bo'limiga muvofiq nazorat stendlarida va sinov rejimida sinovdan o'tkazilishi kerak.

20. Tarmoqlararo ekranning ishlashi (xizmati, sozlamalarini o'zgartirish) Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoya qilish boshqarmasi tomonidan amalga oshiriladi.

V. Tarmoqlararo ekranlarning sozlamalariga o'zgartirish kiritish tartibi

21. Tarmoqlararo ekran sozlamalariga o'zgartirishlar quyidagi hollarda ularga xizmat ko'rsatadigan Xavfsizlik va axborotlarni muhofaza qilish departamenti Axborotlarni muhofaza qilish boshqarmasi mutaxassislari tomonidan amalga oshiriladi:

filtrlash qoidalarini o'zgartirish yoki alohida ulanishlar va kirishga cheklovlar o'rnatish zarurati mavjud bo'lgan taqdirda rahbariyatning buyrug'iga binoan yoki siyosatga asosan o'zgartirish kiritiladi;

lokal tarmoq, korporativ tarmoq segmenti konfiguratsiyasidagi o'zgarishlar, yangi axborotlashtirish obyektlarini ulash, yangi ilovalar, qurilmalar yoki foydalanuvchilarni qo'shish;

bankning tarkibiy bo'linmasi rahbarining Xavfsizlik va axborotni muhofaza qilish departamenti direktori nomiga tarmoqlararo ekran o'zgartirishlar kiritish zarurligi to'g'risidagi arizasi asosida taqdim etadi;

nosozliklar yuzaga kelishi yoki bosqinchilarning hujumlarini aniqlash va h.k.

22. Tarmoqlararo ekran konfiguratsiyasiga o'zgartirishlar quyidagi hollarda ularga xizmat ko'rsatuvchi mutaxassislar tomonidan amalga oshiriladi:

tarmoqlararo ekranning ish faoliyatini modernizatsiya qilish va yaxshilash zarurati;

tarmoqlararo ekrani elementlarining ishlamay qolishi.

23. Tarmoqlararo ekran dasturiy ta'minotiga o'zgartirishlar faqat dasturiy ta'minot ishlab chiqaruvchi tomonidan yangilangan taqdirdagina amalga oshiriladi. Tarmoqlararo ekran dasturiy ta'minotini yangilash siyosatga 6-ilovada keltirilgan Tizim va amaliy dasturiy ta'minotni yangilash, shuningdek, ma'lumotlarni zaxiralash va tiklash to'g'risidagi nizomga muvofiq amalga oshiriladi.

24. Tarmoqlararo ekran sozlamalariga o'zgartirishlar kiritish uchun arizada

unga kirish huquqlarini o'zgartirishni talab qiladigan texnologiyaning (axborot tizimi, resurs va boshqalar) qisqacha tavsifi, shuningdek, foydalanish muddatini bu o'zgarishlar qanday amalga oshiriladi (agar kerak bo'lsa)ko'rsatadi.

Texnologiya muddatidan oldin to'xtatilgan taqdirda, ushbu texnologiyaga xizmat ko'rsatuvchi bankning tarkibiy bo'linmasi boshlig'i Xavfsizlik va axborotlarni muhofaza qilish departamentini o'z vaqtida xabardor qilishi shart.

25. Tarmoqlararo ekranning sozlamalari va konfiguratsiyasiga kiritilgan har bir o'zgartirish, ularga xizmat ko'rsatuvchi administratorlar Axborotlarni muhofaza qilish boshqarmasi boshlig'i va/yoki Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori bilan kelishib olishlari va tasdiqlashlari kerak.

26. Tarmoqlararo ekranga kiritilgan o'zgarishlarni qayd qilish tarmoqlararo ekranning jurnal fayllarini qayd qilish orqali amalga oshirilishi kerak.

Shuningdek, tarmoqlararo ekranning sozlamalari va konfiguratsiyasiga kiritilgan o'zgartirishlar administratorlar tomonidan jurnallarda qayd etilishi kerak, ularning shakli nizomning ilovasida keltirilgan.

27. Xavfsizlik va axborotlarni muhofaza qilish departamentining alohida tayinlangan a'zosi, tarmoqlararo ekran administratori bo'lmagan, har oy tarmoqlararo ekran sozlamalari va konfiguratsiyasiga kiritilgan o'zgarishlarni tarmoqlararo ekran administrator tomonidan faoliyati jurnali (jurnal fayllari) bilan tarmoqlararo ekranni o'zgartirish jurnalini ko'rib chiqish orqali tekshirishi kerak.

28. Shuningdek, Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi kamida uch oyda bir marta tarmoqlararo ekran sozlamalarini tekshirish va nazorat qilishni amalga oshiradi. Audit davomida tarmoqlararo ekranning ishlashiga qo'yiladigan talablarga muvofiqligi, sozlamalarning to'g'riligi, shuningdek, ro'yxatga olish va tizim jurnallarini (jurnal fayllari) ko'rish tekshiriladi.

VI. Tarmoqlararo ekranni sinovdan o‘tkazish tartibi

29. Tarmoqlararo ekranni sinovdan o‘tkazishning maqsadi ushbu dasturiy-apparat vositaning (paket filtrlari, proksi-serverlari, dastur shlyuzlari) tartibga soluvchi me’yoriy hujjatlar talablarga muvofiqligini tasdiqlash, shuningdek filtrlashning talab qilingan qoidalarini bajarilishini tekshirish hisoblanadi.

30. Tarmoqlararo ekranni sinovdan o‘tkazish uchun boshqaruv xavfsizligi stendi yaratilib, u axborot xavfsizligi administratoriga o‘zboshimchalik bilan paket yaratishga (ulanishni o‘rnatishga) va tarmoqlararo ekran sozlamalarining sinov natijalariga (tarmoqlararo ekrani orqali paket o‘tganligi yoki ulanish o‘rnatilganligi) tahlil qilishga imkoniyatini beradi.

Eng oddiy sinov bu paket (ulanish) generatori va trafikni tekshirgich kiradi. Ulanish o‘rnatilishini tekshirish uchun paket generatori ulanishni o‘rnatishi kerak va trafik tekshirgichi har qanday o‘zboshimchalik bilan belgilangan port yoki dasturga xizmat ko‘rsatadigan universal server bo‘lishi kerak.

31. Sinov jarayonida axborot xavfsizligi administratori paketni uzatish yoki tarmoqlararo ekranni “turli tomonlarida” ulanishni o‘rnatish natijalarini yaratishi va tahlil qilishi kerak (ya’ni paket generatori va trafik analizatori turli yo‘nalishlarda joylashgan bo‘lishi kerak).

Tarmoqlararo ekran orqali o‘tkazilgan sinov trafiklari natijalarini tahlil qilish va ularning aniq talabga javob beradigan deb hisoblangan natijalar bilan taqqoslash asosida tarmoqlararo ekran sinovdan o‘tgan xavfsizlik mexanizmining to‘g‘ri bajarilishi to‘g‘risida xulosa chiqariladi.

32. Tarmoqlararo ekran sinovi barcha monitoring funksiyalari va filtrlash qoidalari tasdiqlanmaguncha amalga oshiriladi. Tarmoqlararo ekran sinov muddati kamida bir oy bo‘lishi kerak.

33. Sinov va tajribadan muvaffaqiyatli o'tgandan so'ng, tarmoqlararo ekran ishlashga ruxsat etiladi.

VII. Tarmoqlararo ekranni o‘rnatish va ishlatish tartibi

34. Tarmoqlararo ekranni ulashdan oldin nizom va siyosat talablariga muvofiq sozlanishi kerak.

35. Tarmoqlararo ekran bilan ishlashda quyidagilar ta'minlanishi kerak:

tarmoqlararo ekrandan chiqish ma'lumotlari va jurnal fayllarini doimiy monitoring qilish;

tarmoqlararo ekranning ishlashini tizimli monitoring qilish va diagnostika qilish, shuningdek tarmoqlararo ekrani tomonidan nazorat funksiyalarini bajarishni nazorat qilish;

tarmoqlararo ekran dasturini yangilash;

qoidalarning 5-bo'limida ko'rsatilgan hollarda tarmoqlararo ekranning sozlamalari va konfiguratsiyasini o'zgartirish;

filtrlash va boshqarish funksiyalarini bajarish uchun belgilangan talablarga muvofiqligi uchun tarmoqlararo ekran sozlamalari va konfiguratsiyasini har kuni tekshirish;

tarmoqlararo ekranning so'nggi sozlamalarini saqlash (elektron sozlamalar arxivini yaratish);

tarmoqlararo ekranning ishlashidagi nosozliklar aniqlangan taqdirda ularni bartaraf etish;

sovuq zaxiradagi tarmoqlararo ekranning ishlashini tekshirish va asosiy tarmoqlararo ekran ishlamay qolganda uni faollashtirish

barcha so'nggi sozlamalar va konfiguratsiyalarni tiklash bilan tarmoqlararo ekran ishlamay qolganda ishlashni tiklash.

36. Trafik hajmi oshishi yoki tarmoqlararo ekran ishlamay qolishi va boshqalar holatida tarmoqlararo ekranlarining ish tartibiga o‘zgartirishlar kiritilishi mumkin.

37. Tarmoqlararo ekranning ishlashiga o‘zgartirishlar Axborotlarni muhofaza qilish boshqarmasi tomonidan Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori bilan kelishilgan holda kiritiladi va tarmoqlararo ekranga xizmat ko‘rsatuvchi administratorlar tomonidan amalga oshirilishi kerak.

38. Tarmoqlararo ekran administratorlari har kuni xavfsizlik jurnallari va tarmoqlararo ekran hodisalari statistikasini ko'rib chiqishlari va tashqi hujumlarni aniqlash uchun tarmoqlararo ekran elektron jurnallarini tahlil qilishlari kerak.

39. Agar tashqi hujumlar aniqlansa, tarmoqlararo ekranni javobgar administratorlar tomonidan Xavfsizlik va axborotlarni muhofaza qilish

departamentining Axborot xavfsizligi boshqarmasiga xabar berishlari shart.

Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi barcha aniqlangan tashqi hujumlari to‘g‘risida tashqi hujumlar aniqlangan kunning o‘zida Markaziy bankka xabar berishi shart.

VIII. Javobgarlik

40. Nizom da belgilangan talablarga rioya etilishi uchun tarmoqlararo ekranni yurituvchi va ekspluatatsiya qiluvchi administratorlar, shuningdek, Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi boshlig‘i javobgardir.

41. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi ushbu nizom talablariga rioya etilishini nazorat qiladi.

Tarmoqlararo ekran va tarmoq infratuzilmasi darajasida axborot xavfsizligini ta’minlash to’g’risidagi nizom ga ilova

Tarmoqlararo ekran sozlamalari va konfiguratsiyasiga kiritilgan o‘zgartirishlarni qayd qilish JURNALI

№	Sana va vaqt	Kiritilgan o‘zgartirish	O’zgartirish kiritish sababi

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
3-ilova

Korporativ tarmoq administratori yo’riqnomasi

I. Umumiy qoidalar

1. Ushbu yo‘riqnoma “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank) korporativ tarmog‘ini boshqarish tartibi va qoidalarini, shuningdek korporativ tarmoq administratoriga tarmoqning uzluksiz ishlashini ta’minlash va axborot xavfsizligini tegishli darajada ushlab turish majburiyatini belgilash uchun ishlab chiqilgan.

2. Korporativ tarmoq administratorligi bo‘yicha mas’uliyatlar korporativ tarmoq administratoriga (keyingi o‘rinlarda - tarmoq administratori), u bo‘lmaganda esa Axborot texnologiyalar departamentining Telekommunikatsiya va aloqa bo’limi xodimlari bo‘lgan tarmoq administratorining o‘rinbosariga yuklanadi. Bank rahbariyatining buyrug‘i bilan tayinlanadi.

3. Tarmoq administratorining huquq va majburiyatlari ushbu yo‘riqnoma bilan belgilanadi va uning lavozim yo‘riqnomasida ko‘rsatiladi.

Tarmoq administratori kasallik tufayli ish joyida bo'lmagan davrida yoki mehnat ta'tilida va xizmat safarida bo'lgan davrda tarmoq administratorini ushbu Yo'riqnomada belgilangan huquqlari va majburiyatlari uning o'rinbosari zimmasiga yuklanadi.

4. Tarmoq administratorlari oliy ma’lumotga ega va AKT sohasida kamida 3 yil ish tajribasiga ega bo‘lishi kerak.

5. Tarmoq administratorining talablari va uning yo'qligida tarmoq administratorining o'rinbosari o'z funksiyalarini bajarishi bilan bog'liq talablari korporativ tarmoqning barcha foydalanuvchilari, shuningdek korporativ tarmoqning bir qismi bo'lgan tarmoqlararo ekran tarmoq uskunalarining ishlashini ta'minlaydigan xodimlar uchun majburiydir.

6. Tarmoq administratori quyidagilarga asoslangan holda ish yuritadi:

Axborot xavfsizligi siyosati;

bankning buyruqlari va farmoyishlari;

qonun hujjatlari, ichki mehnat qoidalari;

korporativ tarmoqlarni boshqarish va axborot xavfsizligini ta’minlash usullari va qo‘llanmalari;

va ushbu yo‘riqnomaga asosan.

II. Vazifalari

7. Tarmoq administratorining vazifalariga quyidagilar kiradi:

korporativ tarmoqning normal ishlashi va axborot xavfsizligini ta'minlash;

korporativ tarmoqda xavfsiz ulanishlarni tashkil etish va ta'minlash.

III. Majburiyatlari

8. Tarmoq administratori quyidagilarni bilishi kerak:

korporativ tarmog‘ida axborot texnologiyalaridan mukammal foydalanish;

korporativ tarmoq uskunalarining foydalanish qo‘llanmalari;

korporativ tarmoqning topologiyasi va tashkil etish sxemasi;

korporativ tarmoqning axborot xavfsizligini ta’minlashga qo‘yiladigan talablar;

korporativ tarmoqdagi ma’lumotlarning chiqib ketish kanallarini aniqlash usullari;

korporativ tarmoqda xavfsiz ulanishni tashkil etish bo‘yicha ishlarni rejalashtirish va o‘tkazish usullari;

tarmoq qurilmalari va tarmoq oqimlarini boshqarish usullari va texnologiyalari;

mehnatni muhofaza qilish qoidalari, normalari, xavfsizlik choralari va yong‘indan himoya qilish.

9. Korporativ tarmoqning normal ishlashi va axborot xavfsizligini ta'minlash uchun tarmoq administratori korporativ tarmoq tarkibiga kiruvchi tarmoq uskunasiga texnik xizmat ko'rsatish uchun mas'ul bo'lgan MBXOning Axborot texnologiyalari bo'limlari Telekommunikatsiya va aloqa bo’limi xodimlar, shuningdek, bo'ysunuvchi BXMdagi mas’ullar ishini tashkil qiladi va muvofiqlashtiradi.

10. Tarmoq administratori quyidagilarga majbur:

korporativ tarmoq tarkibiga kiruvchi tarmoq uskunalariga xizmat ko‘rsatishda Axborot texnologiyalari departamentining Telekommunikatsiya va aloqa bo‘limi xodimlarining harakatlarini nazorat qilish;

yangi tarkibiy bo'linmalar va axborotlashtirish obyektlarini korporativ tarmoqqa ulashni tashkil etish va ta'minlash;

korporativ tarmoqni modernizatsiya qilish va rivojlantirish rejalarining bajarilishini ta'minlash;

korporativ tarmoq kanallari, tashqi kanallar va uchinchi tomon axborot tizimlariga ulanish uchun tashkil etilgan kanallar orqali tarmoq trafigini taqsimlashni (boshqarishni) ta’minlash, shuningdek marshrutlash jadvalini boshqarish;

Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi bilan hamkorlikda korporativ tarmoqning tashqi tarmoqlarga xavfsiz ulanishini ta’minlash;

korporativ tarmoq tarkibiga kiruvchi texnik, dasturiy, tarmoq resurslarining ishlashini nazorat qilish;

korporativ tarmoqning zarur apparat va dasturiy ta’minotini o‘rnatish, sozlash ishlarini tashkil etish va amalga oshirish;

korporativ tarmoq tarkibiga kiruvchi apparat - dasturiy ta'minot, tarmoq resurslarining ishlashi (o'rnatish, sozlash, boshqarish va texnik xizmat ko'rsatish) ustidan nazoratni amalga oshirish;

korporativ tarmoqqa profilaktik xizmat ko‘rsatish jadvallarini ishlab chiqish va amalga oshirish;

kabel infratuzilmasini qo'llab-quvvatlash bo'yicha ishlarni tashkil etish va amalga oshirish, shu jumladan. tarmoq qurilmalari va axborotni qayta ishlash vositalarini korporativ tarmoqqa ulash, kabel tizimidagi buzilishlarni izlash va tuzatish;

korporativ tarmoq faoliyatidagi turli og‘ishlarni o‘z vaqtida bartaraf etish bo‘yicha ishlarni aniqlash va amalga oshirish;

korporativ tarmoqda axborot xavfsizligi buzilishi bilan bog‘liq hodisalarga tezkor va samarali javob berish;

himoya talablarining mumkin bo'lgan buzilishlarini aniqlash uchun korporativ tarmoq jurnallari ma'lumotlarini tahlil qilish;

korporativ tarmoq vositalari va jihozlarining jismoniy xavfsizligini nazorat qilish;

ruxsatsiz shaxslarning korporativ tarmoqqa ulanishini, shuningdek korporativ tarmoq serverlari va tarmoq uskunalarida ishlashini oldini olish;

ijaraga olingan ma’lumotlarni uzatish kanallari va korporativ tarmoqni tashqi tarmoqqa va uchinchi shaxslarning axborot tizimlariga ulaydigan kanallarning uzluksiz ishlashini ta’minlash maqsadida aloqa operatorlari bilan o‘zaro hamkorlik qilish;

vaqti-vaqti bilan kamida oyiga bir marta korporativ tarmoqning tarmoq uskunalarini nazorat qilish tekshiruvlarini o'tkazish, ularning to'g'ri ishlashini tekshirish. Belgilangan tekshirishlar va sinovlar Axborot texnologiyalari departamenti direktori tomonidan tasdiqlanadigan profilaktika ishlari jadvaliga muvofiq amalga oshiriladi;

korporativ tarmoq infratuzilmasini rivojlantirish hamda uning xavfsizlik va ishonchlilik darajasini oshirish bo‘yicha takliflar tayyorlash va kiritish;

korporativ tarmoq tarmoq uskunasining oxirgi sozlamalarini muntazam zaxiraviy nusxasini, shuningdek, asosiy tarmoq uskunasining zaxira nusxasini yaratish;

har oy Axborot texnologiyalari departamentining Axborot texnologiyalari infratuzilmasini rivojlantirish va qo‘llab-quvvatlash boshqarmasi boshlig‘iga korporativ tarmoqning foydalanuvchilar faoliyat ko‘rsatishi va axborot xavfsizligi holati to‘g‘risida, shuningdek favqulodda vaziyatlar va axborotni himoya qilish bo‘yicha belgilangan talablarning buzilishi holatlari to‘g‘risida zudlik bilan hisobot taqdim etish;

korporativ tarmoqda axborot xavfsizligini ta’minlash bo‘yicha turli hodisalar yuz berganligi to‘g‘risida Xavfsizlik va axborotlarni muhofaza qilish departamentini xabardor qilish va ularning oqibatlarini bartaraf etish va ish faoliyatini tiklash bo‘yicha kelishilgan harakatlarni amalga oshirish;

bank xodimlari tomonidan korporativ tarmoqdan foydalanishda mazkur siyosat talablarining bajarilishi ustidan nazoratni ta’minlash.

11. Tarmoq administratori va korporativ tarmoqning tarmoq uskunasidan foydalanuvchi xodimlarga quyidagilar taqiqlanadi:

ish joylarini nazoratsiz, shu jumladan ish holatida qoldirish;

tarmoq uskunasining konfiguratsiyasi va sozlamalari haqidagi ma'lumotlarni oshkor qilish;

istalgan ommaviy axborot vositalarida korporativ tarmoq

foydalanuvchilarining parollarini uzatish, shuningdek, ularni xodimlarning o'zidan boshqa har kimga yetkazish.

IV. Huquqlari

12. Tarmoq administratori quyidagi huquqlarga ega:

korporativ tarmoqning har qanday tekshiruvlarida qatnashish;

bank korporativ tarmog‘ining ishlashi va rivojlanishini ta’minlash bo‘yicha rahbariyat tomonidan qabul qilingan qarorlari loyihalari bilan tanishish;

korporativ tarmoqda axborot xavfsizligini ta’minlash hamda foydalanuvchilarning axborot tizimlari, resurslari va tashqi tarmoqlarga kirishini boshqarish masalalari bo‘yicha Xavfsizlik va axborotlarni muhofaza qilish departamenti bilan o‘zaro hamkorlik qilish;

bank tizimi administratori bilan bank xodimlarini korporativ tarmoqqa ulash va kirishini boshqarish masalalari bo‘yicha o‘zaro hamkorlik qilish;

korporativ tarmoqning ishni takomillashtirish, tarmoq uskunalarini zaxira qilish va axborot xavfsizligini ta'minlash bo'yicha takliflar kiritish;

bankning korporativ tarmog‘idan foydalanish qoidalarini Axborot texnologiyalaridan departamenti direktori bilan kelishilgan holda belgilash va o‘zgartirish;

bank mablag‘lari hisobidan malaka oshirish.

V. Javobgarlik

13. Tarmoq administratori quyidagi hollarda javobgarlikka tortiladi:

yo‘riqnomada nazarda tutilgan o‘z vazifalarini bajarmaganligi yoki lozim darajada bajarmaganligi;

bank korporativ tarmoqlaridan foydalanishda foydalanuvchilarning xatti-harakatlarini boshqarish bo‘yicha u tomonidan olib borilayotgan ishlarning sifatsizligi;

texnika xavfsizligi qoidalarini buzilishiga javobgardir.

14. Tarmoq administratori o'z vazifalarini bajarmaganligi yoki lozim darajada bajarmaganligi uchun intizomiy yoki boshqa jazolarga tortilishi mumkin.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
4-ilova

Xavfsizlik va axborotlarni muhofaza qilish departamenti to'g'risidagi nizom

I. Umumiy qoidalar

1. Mazkur nizom “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank) Xavfsizlik va axborotlarni muhofaza qilish departamenti (keyingi o‘rinlarda- Departament deb yuritiladi) va uning tarkibiy bo‘linmalarining vakolatlari, majburiyatlari, huquq va majburiyatlarini belgilash maqsadida ishlab chiqilgan.

2. Bankda axborot xavfsizligini ta’minlash bo‘yicha ishlarni tashkil etish va muvofiqlashtirish departamentga yuklatilgan.

3. Departamentning asosiy yo’nalishi bankning barqaror faoliyatini ta'minlash, uning xavfsizligiga tahdid qiluvchi omillarini oldini olish, qonuniy manfaatlarini noqonuniy tajovuzlardan, xodimlarning hayoti va sog'lig'ini bankning moliyaviy va moddiy-texnik vositalarni o'g'irlashni oldini olish hamda axborot tizimlari va tarmoqlaridagi ma'lumotlarni buzilishi va yo'q qilinishini oldini olishdan iborat.

4. Departament bankning mustaqil tarkibiy bo‘linmasi hisoblanadi.

5. Departament direktori bank boshqaruvi Raisining buyrug‘i bilan ishga qabul qilinadi hamda ushbu departamentga rahbarlik qiladi, shuningdek amaldagi qonunchilikka binoan lavozimdan ozod qilinadi.

6. Departament direktori oliy ma’lumotli va rahbarlik lavozimlarida kamida 5 yillik ish tajribasiga ega bo‘lishi kerak.

7. Departament direktori bevosita bank boshqaruvi Raisiga bo‘ysunadi va departament zimmasiga yuklangan vazifalar va funksiyalarning muvaffaqiyatli bajarilishi uchun shaxsan javobgardir.

8. Departament direktori bo‘lmagan davrda (ta’tilda, kasallikda, xizmat safarida va h.k.) uning vazifalari bank boshqaruvi Raisi buyrug‘i bilan vaqtincha direktor o‘rinbosari zimmasiga yuklanadi.

9. Departamentning tashkiliy tuzilmasi quyidagilardan iborat:

1) Bank xavfsizligi boshqarmasi:

Bank xavfsizligi bo’limi;

Axborot-tahlil bo'limi;

2) Axborotlarni muhofaza qilish boshqarmasi:

Axborot va kartochkalar tizimi xavfsizligi bo’limi;

Elektron kalitlarni ro'yxatga olish bo'limi;

10. Departamentning tarkibiy bo‘linmalari faoliyatiga rahbarlikni ularning boshliqlari amalga oshiradi.

11. Departament tuzilmasi va shtat jadvali bank boshqaruvi Raisi tomonidan tasdiqlanadi.

12. Departament va uning tarkibiy bo'linmalarining vazifalari ushbu nizom bilan belgilanadi va ushbu tarkibiy bo'linmalar to'g'risidagi nizomda belgilab qo'yilgan.

13. Departament xodimlari qonun hujjatlariga muvofiq bank boshqaruvi Raisining buyrug'i bilan Departament direktorining taqdimnomasiga binoan ishga qabul qilinadi va lavozimdan ozod qilinadi.

14. Departamentning shtatdagi lavozimlariga asosan axborot-kommunikatsiya texnologiyalari sohasi mutaxassislari, huquqni muhofaza qilish organlari va O'zbekiston Respublikasi Qurolli Kuchlarining sobiq xodimlari, shaxsiy va ishbilarmonlik fazilatlari, kasbiy mahorati va sog'lig'i holati, bank axborot xavfsizligi va himoyasini ta'minlash bo'yicha ishlarni bajarishga qodirlarni qabul qiladi.

Ayrim hollarda oliy ma'lumotga ega bo'lmagan, lekin zarur kasbiy tajribaga ega bo'lgan, o'z zimmasiga yuklangan vazifalarni to'liq va samarali bajarishga qodir bo'lgan fuqarolar Departament tomonidan ishga qabul qilinishi mumkin.

15. Departament xodimi ishda bo'lmagan davrda (ta'til, kasallik, xizmat safari va h.k.) uning vazifalari Departament direktorining qarori bilan vaqtincha uning o'rnini bosuvchi boshqa xodimga yuklanadi.

16. Axborotlarni muhofaza qilish boshqarmasi xodimlari o'z faoliyatida quyidagilarga rahbarlik qiladilar:

bankning axborot xavfsizligi siyosati;

axborot xavfsizligi sohasidagi normativ-huquqiy dalolatnomalar va normativ hujjatlar;

bankning buyruqlari va farmoyishlari;

qonun hujjatlari, ichki mehnat qoidalari;

ushbu nizomga asosan.

II. Asosiy vazifalari

17. Axborot xavfsizligini ta'minlash bo'yicha departament va uning bo'limlari bilan Axborotlarni muhofaza qilish boshqarmasining asosiy vazifalari quyidagilardan iborat:

1) Bankning axborot xavfsizligini ta'minlash sohasida normativ-huquqiy qo'llab-quvvatlash chora-tadbirlarini amalga oshirish;

2) Bank axborot aktivlarini boshqarish bo'yicha chora-tadbirlarni amalga oshirish;

3) xodimlarning xavfsizligini ta'minlash bo'yicha chora-tadbirlarni amalga oshirish, ularni xabardor qilish, axborot xavfsizligi sohasida o'qitish va malakasini oshirish;

4) Bankda axborotning texnik va kriptografik himoyasini ta'minlash bo'yicha ishlarni tashkil etish va amalga oshirish;

5) Bank axborotlashtirish obyektlari xavfsizligi holatini nazorat qilish va baholash;

6) Bankda axborot xavfsizligi hodisalariga qarshi kurashish bo'yicha tadbirlarni tashkil etish va o'tkazish;

7) Bank axborotlashtirish obyektlarining uzluksiz ishlashi va qayta

tiklanishi bo‘yicha chora-tadbirlarni ta’minlash, shuningdek, favqulodda va avariya vaziyatlarda tiklash ishlarini tashkil etish va o‘tkazish ustidan nazoratni amalga oshirish;

8) Bank axborot xavfsizligi siyosatining dolzarbligi va samaradorligini baholash;

9) axborot xavfsizligiga yuzaga kelishi mumkin bo‘lgan tahdidlarni bashorat qilish va ularning oldini olish, shuningdek, Bankda axborot xavfsizligini ta’minlash holatini tahlil qilish bo‘yicha tadqiqotlar va tashviqotlar o‘tkazish.

18. Moddiy resurslar va boyliklarning yaxlitligi va saqlanishini, bank obyektlariga xavfsiz jismoniy kirish rejimini, shuningdek, Bankda yong‘in xavfsizligini (keyingi o‘rinlarda bank xavfsizligi deb yuritiladi) ta’minlash bo‘yicha asosiy vazifalar Departamenti va uning tarkibiga kiruvchi bank xavfsizligi boshqarmasi uning bo‘limlari bilan:

1) Bankda bank xavfsizligi choralarini amalga oshirish;

2) Bank obyektlarida bank xavfsizligi talablariga rioya etilishini ishlab chiqish va nazorat qilish;

3) Bank obyektlarini jismoniy va yong‘in xavfsizligini ta’minlovchi texnik vositalar bilan jihozlash, shuningdek ularning ishlashini ta’minlash;

4) favqulodda vaziyatlarning oldini olish va ularni bartaraf etish, xodimlarning xavfsizligini ta'minlash va ular yuzaga kelgan taqdirda Bankka yetkaziladigan zararni kamaytirish tizimi faoliyatini tashkil etish.

5) Bank xavfsizligiga yuzaga kelishi mumkin bo‘lgan tahdidlarni bashorat qilish va oldini olish bo‘yicha tadqiqotlar va tashviqotlar o‘tkazish, shuningdek, Bankda bank xavfsizligini ta’minlash holatini tahlil qilish.

III. Vazifalari

19. Axborot xavfsizligini ta'minlash bo'yicha departamentning vazifalariga quyidagilar kiradi:

1) Axborot xavfsizligi sohasida normativ-huquqiy yordam:

bankning axborot xavfsizligi sohasida ichki hujjatlarini ishlab chiqish;

bankning axborot xavfsizligi sohasida normativ-huquqiy bazasini shakllantirish va yuritish;

axborot xavfsizligini ta’minlash bo‘yicha ichki me’yoriy hujjatlarni takomillashtirish bo‘yicha takliflar ishlab chiqish va bank boshqaruviga ko‘rib chiqish uchun kiritish;

axborot xavfsizligi sohasidagi normativ hujjatlar talablarini bank xodimlariga yetkazish;

bankda axborot xavfsizligini ta’minlash bo‘yicha chora-tadbirlar rejalarini ishlab chiqish.

2) Axborot aktivlarini boshqarish:

bankning konfidensial ma’lumotlar ro‘yxati va axborot aktivlari reestrini yangilash, axborot hamda axborot resurslarini kategoriyalash bo‘yicha ishlarni tashkil etish va amalga oshirish;

inventarizatsiya o'tkazish, axborot aktivlari va himoya qilish obyektlari ro'yxatini aniqlash va yuritish, ularni xavfsizlik darajasi bo'yicha tasniflash, muhim

va asosiy himoya qilish obyektlariga nisbatan tahdid modelini aniqlash;

axborot tizimlariga va boshqa himoya qilish obyektlariga kirish huquqiga ega bo'lgan xodimlarning ro'yxatini tuzish, shuningdek ularning kirishini nazorat qilish;

bank axborot resurslari reyestriga kiritilgan axborot aktivlarini etiketlash, ulardan foydalanish va axborot xavfsizligini ta'minlash talablariga rioya etilishini nazorat qilish;

bank xodimlari uchun buxgalteriya hisob ining saqlaydigan va tashuvchi vositalar va ma'lumotlar disklarini tegishli tashkiliy-ma'muriy hujjatlar bilan ta'minlash;

konfidensial ma'lumotlar uchun foydalaniladigan ma'lumot tashuvchi va saqlovchi vositalar ro'yhatini yuritish.

3) Xodimlarning xavfsizligi, xabardorligi, o'qitish:

bank xodimlarini mazkur siyosat, shuningdek, Internet tarmog'i va axborotni kriptografik himoyalash vositalaridan foydalanishdagi majburiyatlari (keyingi o'rinlarda AKH deb yuritiladi) bilan tanishtirish;

axborot xavfsizligi masalalari bo'yicha bank xodimlarini o'qitish (axborotlash), treninglar va seminarlar (o'qitish), attestatsiyadan o'tkazish, testdan o'tkazish yoki so'rov (baholash)ni tashkil etish va o'tkazish;

bank xodimlarini axborot xavfsizligini ta'minlash bo'yicha tashkiliy-ma'muriy hujjatlar bilan tanishish va o'rganish bo'yicha o'quv mashg'ulotlarini tashkil etish;

bankning axborot xavfsizligini ta'minlashga mas'ul mutaxassislari uchun malaka oshirish kurslarini tashkil etish;

bank tarkibiy bo'linmalari va xodimlariga axborot xavfsizligini ta'minlash masalalarida uslubiy va amaliy yordam ko'rsatish.

4) Axborotni texnik va kriptografik himoya qilish:

bank axborot himoyasi va axborot tizimlari himoyasini ta'minlash, shuningdek Bankda axborot xavfsizligi tizimini tashkil etish, shu jumladan, Bankda axborotni kriptografik himoyalashni ta'minlash bo'yicha talablarni ishlab chiqish;

axborot xavfsizligi tizimini joriy etish va rivojlantirish bo'yicha amaliy chora-tadbirlarni rejalashtirish va amalga oshirish;

sotib olingan texnik va kriptografik axborotni himoya qilish vositalariga qo'yiladigan texnik talablarni aniqlash;

bank axborotni himoya qilish tizimini joriy etish va rivojlantirish bo'yicha chora-tadbirlarni amalga oshirish doirasida axborotni himoya qilishning texnik va kriptografik vositalarini xarid qilishni tashkil etish;

binolarni ajratish, foydalanish ko'rsatmalari va texnik xizmat ko'rsatish qoidalarini qo'llashni o'z ichiga olgan tizim va axborot xavfsizligi vositalarini joriy etish va saqlashga tayyorgarlik ko'rish bo'yicha tashkiliy chora-tadbirlarni amalga oshirish;

axborot xavfsizligi vositalarini joriy etish jarayonida tajriba-ekspluatatsion va qabul qilish sinovlarini o'tkazish;

himoya qilish tizimi va uning texnik va kriptografik himoya vositalarining ishlashi (boshqarilishi) uchun mas'ul xodimlarni aniqlash;

axborot xavfsizligi vositalarini (tarmoqlararo ekran, IDPS vositalari, DLP

tizimi, antivirus vositasi, xavfsizlikni tahlil qilish va boshqarish vositalari, PAM tizimi, ERI kalitlarini ro'yxatga olish markazi va boshqalar) boshqarish (boshqaruv), shu jumladan konfiguratsiyani boshqarish va ularning sozlamalari, tiklash faoliyatni saqlash, dasturiy ta'minot yangilanishlarini o'rnatish, operatsion hujjatlarni sozlash, xavfsizlik hodisalarini nazorat qilish, nazorat qilish tartiblari va natijalarini hujjatlashtirish;

bank xodimlarining internet tarmog‘iga kirishini ta’minlash bo‘yicha arizalarni qabul qilish, ko‘rib chiqish va tasdiqlash, shuningdek ularning internet tarmog‘idan foydalanishini nazorat qilish;

bankning axborot va unga ishlov berish jarayonlari xavfsizligini ta’minlash nuqtai nazaridan apparat-dasturiy vositalarini o‘rnatish va modernizatsiya qilish tartibini belgilash va qayta ko‘rib chiqish;

axborot va uni qayta ishlash jarayonlari xavfsizligini ta'minlash nuqtai nazaridan dasturiy ta'minotni loyihalash, ishlab chiqish, diskni koddan chiqarish, sinovdan o'tkazish, joriy etish va ulardan foydalanish tartibini aniqlash va qayta ko'rib chiqish;

bankda axborotni kriptografik himoyalash vositalarini (keyingi o‘rinlarda - AKH) va elektron raqamli imzo vositalarini (keyingi o‘rinlarda - ERI deb yuritiladi) joriy etish bo‘yicha amaliy chora-tadbirlarni rejalashtirish va amalga oshirish;

bank xodimlari va internet-Banking va mobil Banking mijozi uchun ERI kriptografik kalitlari, ERI ochiq kalitlari sertifikatlarini shakllantirish;

bank xodimlari va internet-Banking va mobil Banking mijoziga ERI kriptografik kalitlarini shakllantirish jarayonlarini tartibga solish va ta'minlash;

bank xodimlari tomonidan ERI kriptografik kalitlari xavfsizligiga talablarni aniqlash va nazorat qilish;

ABT foydalanuvchilari bo‘lgan bank xodimlarining, shuningdek, internet-Banking va mobil Banking mijozlarining ERI ochiq kalitlari sertifikatlarining amal qilishini to‘xtatib turish va bekor qilish;

kriptografik shifrlash kalitlari va ERIning xavfsiz USB-tashuvchilari hisobini yuritish;

bankda qonun hujjatlarida belgilangan tartibda sertifikatlangan AKHdan foydalanish bo‘yicha talablarning bajarilishi;

bank boshqaruvi faoliyati va xavfsizligini ta’minlashda kamchiliklar aniqlangan taqdirda axborot xavfsizligi tizimini takomillashtirish bo‘yicha takliflar tayyorlash va rahbariyatiga taqdim etish.

5) Xavfsizlik holatini nazorat qilish va baholash:

bankda axborot xavfsizligi risklarini tahlil qilish va baholash;

xavfsizlikni tahlil qilish va nazorat qilish vositalaridan foydalangan holda axborotni texnik va kriptografik himoya qilish bo'yicha chora-tadbirlar ko'rilishini tekshirish, xavfsizlikni baholash va himoyalangan obyektlardagi zaifliklar va sizib chiqish kanallarini aniqlash nuqtai nazaridan ichki auditni tashkil etish va o'tkazish;

bank axborotlashtirish obyektlarini akkreditatsiya qilingan tashkilotlar tomonidan tashqi audit va sertifikatlashtirishni tashkil etish;

bank rasmiy web-sayti va boshqa tashqi web-resurslarning axborot xavfsizligi talablariga muvofiqligini tekshirishni tashkil etish;

bankda mavjud axborot tizimlarini, shuningdek, yangidan joriy etilayotgan

axborot tizimlarini modernizatsiya qilish va yangilarini yaratish bo‘yicha texnik shartlarning axborot xavfsizligi talablariga muvofiqligini ekspertizadan o‘tkazishni tashkil etish;

ko'rilgan himoya choralari samaradorligini baholash, shuningdek, audit, ekspertiza va sertifikatlashtirish natijalari bo'yicha aniqlangan kamchiliklarni bartaraf etish;

bankning axborot xavfsizligini ta’minlash masalalari bo‘yicha uchinchi tomon tashkilotlari bilan tuzilgan shartnoma va kelishuvlarini ekspertizadan o‘tkazish.

6) Axborot xavfsizligi hodisalariga javob:

axborot xavfsizligi hodisalarini aniqlash va tekshirish, shuningdek ularni tahlil qilish va baholash bo'yicha ishlarni tashkil etish va amalga oshirish;

axborot xavfsizligi hodisalarini monitoring qilish va boshqarish tizimlarini, shu jumladan SIEM tizimini administratori (boshqarish);

axborot xavfsizligi hodisalarini hisobga olish va ro'yxatga olish, ular to'g'risida rahbariyatni va manfaatdor shaxslarni xabardor qilish;

axborot xavfsizligi hodisalariga javob berish bo'yicha ishlarni tashkil etish va muvofiqlashtirish, axborot xavfsizligi hodisalari va ularning oqibatlarini bartaraf etish choralarini rejalashtirish va ko'rish;

axborot xavfsizligi hodisalarini tekshirishni tashkil etish va o'tkazish, shuningdek axborot xavfsizligi qoidalarini buzish holatlari bo'yicha ichki tekshiruvlar rahbariyatining ko'rsatmasi bo'yicha;

axborot xavfsizligi hodisalarining takrorlanishining oldini olish choralarini rejalashtirish va ko'rish.

7) Uzluksiz ishlash va tiklash:

axborot xavfsizligi tizimi va uning axborotni himoya qilish vositalarining profilaktika, ta'mirlash va avariya ishlarining reglamentini belgilash va jadvallarini tasdiqlash;

axborot xavfsizligi vositalarining zaxira nusxasini, shuningdek, ularning sozlamalarini zaxiralashni ta'minlash;

Axborot texnologiyalari departamenti tomonidan apparat-dasturiy va dasturiy ta’minotning ortiqcha bo‘lishini ta’minlash, shuningdek, muhim axborotlashtirish obyektlarining dasturiy ta’minoti va ma’lumotlarining zaxira nusxasini yaratish ustidan nazoratni amalga oshirish;

Axborot texnologiyalari departamenti bilan birgalikda avariya holatlar va favqulodda vaziyatlarda o'qitishni tashkil etish;

avariyalar va favqulodda vaziyatlar sodir bo'lgan taqdirda axborotlashtirishning o'ta muhim obyektlarida tiklash ishlarining bajarilishini nazorat qilish.

8) Bank axborot xavfsizligi siyosatining dolzarbligi va samaradorligini baholash:

bank boshqaruviga o‘zgartirish va qo‘shimchalar kiritish yoki siyosatni qayta ko‘rib chiqish zarurligi to‘g‘risida takliflar tayyorlash;

siyosatga o‘zgartirish va qo‘shimchalar kiritish yoki qayta ko‘rib chiqish.

9) Axborot xavfsizligini tadqiq va tahlil qilish:

axborot xavfsizligiga tahdidlarni, ularni amalga oshirishga yordam beruvchi

sabablar va shart-sharoitlarni bartaraf etish chora-tadbirlarini ishlab chiqish va amalga oshirish maqsadida tadqiqotlar o‘tkazish;

axborot xavfsizligini ta’minlash sohasidagi ilg‘or milliy va xorijiy tajriba, usul va vositalarni o‘rganish va ishda foydalanish, shuningdek ulardan Bankda foydalanish imkoniyatlarini ko‘rib chiqish;

bankning axborot xavfsizligini ta'minlash holatini tahlil qilish, tegishli axborot va tahliliy materiallarni tayyorlash;

bank rahbariyatiga hisobot berish uchun Departamentning axborot xavfsizligi faoliyati natijalarini umumlashtirish.

20. Departamentning bank xavfsizligini ta'minlash bo'yicha vazifalariga quyidagilar kiradi:

1) Bank xavfsizligini ta'minlash choralarini ko'rish:

bank binosiga kirishda qo‘riqlash va kirishni nazorat qilishni tashkil etish hamda obyekt ichida kirish nazoratiga rioya etilishini, shuningdek, bank binosi, hududi va xonalari qo‘riqlanishini nazorat qilish;

bosh ofis AB binolari va xonalari xavfsizlik zonalariga bo'lish;

bank binosining qo‘riqlanadigan binolarida axborotlashtirish obyektlari va boshqa moddiy boyliklarni joylashtirish talablarini belgilash va nazorat qilish;

bank xodimlarining hudud va qo'riqlanadigan binolarga jismoniy kirishiga qo'yiladigan talablarni belgilash;

bank xodimlariga kirishni nazorat qilish va boshqarish tizimini (keyingi o'rinlarda ACS deb yuritiladi) joriy etish va ishlatish;

bank bino perimetri, binoga kirish va yo‘laklarni videokuzatuvdan o‘tkazish uchun videokuzatuv tizimini joriy etish va ulardan foydalanish;

himoyalangan binolarga ruxsatsiz jismoniy kirish faktlarini qayd etish uchun qo'riqlash signalizatsiyasi va sensorlarni o'rnatish;

ruxsatnomalar, kalitlar, muhrlar va shtamplarni rasmiylashtirish, hisobga olish, saqlash va yo'q qilish;

xavfli yoki yonuvchan materiallarni muhofaza qilinadigan hududdan yetarlicha masofada xavfsiz saqlashni ta'minlash;

yong'in signalizatsiyasi tizimlari va vositalaridan va yong'inga qarshi uskunalardan foydalanish, shuningdek ularni tegishli joylashtirish;

yong'in sodir bo'lganda avariya chiqishlarini avariya signalizatsiyasi bilan jihozlash, evakuatsiya rejalarini ishlab chiqish;

yong'in xavfsizligi qoidalarini buzishning oldini olish uchun xodimlari o'rtasida profilaktika tadbirlarini o'tkazish;

rahbariyatning ko'rsatmasi bo'yicha bank xavfsizligi qoidalarining buzilishi holatlari yuzasidan ichki tekshiruvlarni tashkil etish va o'tkazish;

bank xavfsizligiga ichki va tashqi tahdidlarni keltirib chiqaradigan faktlar, hodisalar va shaxslar to'g'risidagi ma'lumotlarni qidirish, to'plash, umumlashtirish va tahlil qilish.

2) Bank xavfsizligi talablariga rioya etilishini ishlab chiqish va nazorat qilish:

bank binosi, xizmat ko‘rsatish, texnik va xo‘jalik xonalarining xavfsizligi va yong‘in xavfsizligiga qo‘yiladigan talablarni belgilash;

bankda videokuzatuv tizimi, qo‘riqlash va yong‘in signalizatsiyasi,

shuningdek yong‘in o‘chirish tizimlarini tashkil etishga qo‘yiladigan talablarni ishlab chiqish;

bankning qurilayotgan va rekonstruksiya qilinayotgan obyektlari loyihalarini xavfsizlik talablariga muvofiqligini ekspertizadan o‘tkazish, obyektlarni jismoniy va yong‘in xavfsizligini ta’minlashning texnik vositalari bilan jihozlash bo‘yicha tavsiyalar ishlab chiqish;

loyihalash, qurish va kapital ta'mirlashda sanitariya va yong'in xavfsizligi standartlariga rioya qilish;

bino va hududlarda xavfsizlik va yong'in xavfsizligi talablariga, shuningdek, binolarda videokuzatuv tizimini, xavfsizlik va yong'in signalizatsiya tizimlarini, yong'inni o'chirish tizimlarini tashkil etish talablariga muvofiqligini tekshirish;

loyihalash, montaj qilish va ishga tushirish bosqichlarida bank obyektlarini texnik xavfsizlik tizimlari bilan jihozlash bo'yicha pudratchilar va subpudratchilar tomonidan ishlarning bajarilishini nazorat qilish;

bankning tarkibiy bo‘linmalarining bank xavfsizligini ta’minlash bo‘yicha faoliyatidagi kamchiliklarni aniqlash, ularni bartaraf etish bo‘yicha takliflar ishlab chiqish va kiritish.

3) jismoniy va yong'in xavfsizligini ta'minlashning texnik vositalari bilan jihozlash:

bank binosini muhandislik-texnik vositalar, biometrik identifikatsiyadan o‘tgan kirishni nazorat qilish tizimlari hamda binolar va hududlarga kirishni nazorat qilishning boshqa vositalarini o‘z ichiga olgan jismoniy va yong‘in xavfsizligini ta’minlashning texnik vositalari bilan jihozlash bo‘yicha amaliy chora-tadbirlarni rejalashtirish va amalga oshirish, video kuzatuv, xavfsizlik va yong'in signalizatsiyasi, yong'inni o'chirish vositalari va boshqalar;

bank obyektlarini texnik qo'riqlash uskunalari bilan jihozlash bo'yicha texnik shartlar va talablarni ishlab chiqish, ulardan foydalanish bo'yicha yo'riqnomalarni ishlab chiqishda ishtirok etish;

sotib olingan jismoniy va yong'in xavfsizligi texnik vositalariga texnik talablarni aniqlash;

jismoniy va yong'in xavfsizligini ta'minlash bo'yicha texnik vositalarni xarid qilishni va ularni bank binosi hududlari o'rtasida taqsimlashni tashkil etish;

jismoniy va yong'in xavfsizligini ta'minlashning texnik vositalarining samaradorligini ta'minlash, modernizatsiya qilish va takomillashtirishga qaratilgan ishlarni tashkil etish va bajarilishini nazorat qilish;

dala sharoitida jismoniy va yong'in xavfsizligini ta'minlashning texnik vositalari va jihozlanish darajasini tekshirishni o'tkazish;

kassa punktlarining jihozlanishini ularning qurilmasi va texnik kuchiga qo'yiladigan talablarga muvofiq nazorat qilish.

4) favqulodda vaziyatlarning oldini olish va ularni tugatish:

favqulodda vaziyatlarning oldini olish va bartaraf etish, ular yuzaga kelgan taqdirda bank faoliyatining ishonchliligi va barqarorligini oshirish chora-tadbirlarini ishlab chiqish, tashkil etish va amalga oshirish;

favqulodda vaziyatlarning oldini olish va ularni bartaraf etish bo'yicha tadbirlarni tashkiliy-uslubiy boshqarishni amalga oshirish, ular joylarda yuzaga kelganda bank obyektlari faoliyatining ishonchliligi va barqarorligini oshirish;

boshqaruv va kundalik boshqaruv organlari, obyektlar kuchlari va vositalarining favqulodda vaziyatlarda harakat qilishga tayyorligini nazorat qilish;

bank obyektlarida favqulodda vaziyatlarni bartaraf etish uchun moliyaviy va moddiy resurslar zaxirasini shakllantirish bo'yicha ishlarni tashkil etish;

O‘zbekiston Respublikasi Favqulodda vaziyatlarning oldini olish va harakat qilish davlat tizimining yuqori organlariga favqulodda vaziyatlardan muhofaza qilish sohasidagi axborotni belgilangan tartibda taqdim etish;

huquqni muhofaza qiluvchi organlar bilan birgalikda bankning terrorizmga qarshi himoya darajasini oshirishga qaratilgan profilaktika tadbirlarini tashkil etish;

favqulodda vaziyatlarda bank xodimlarining hayotini ustuvor ta'minlash bo'yicha favqulodda qutqaruv va boshqa ishlarda ishtirok etish.

5) Bank xavfsizligini tadqiq qilish va tahlil qilish:

bank xavfsizligiga tahdidlarni, ularni amalga oshirishga yordam beruvchi sabablar va shart-sharoitlarni bartaraf etish chora-tadbirlarini ishlab chiqish va amalga oshirish maqsadida ilmiy-tadqiqot ishlarini olib borish;

bank xavfsizligini ta’minlash sohasidagi ilg‘or milliy va xorijiy tajriba, usul va vositalarni o‘rganish va ishda foydalanish, shuningdek ulardan Bankda foydalanish imkoniyatlarini ko‘rib chiqish;

bankning xavfsizligini ta'minlash holatini tahlil qilish, tegishli axborot va tahliliy materiallarni tayyorlash;

bank rahbariyatiga hisobot berish uchun bank xavfsizligi boshqarmasi faoliyati natijalarini umumlashtirish.

IV. Huquqlari

21. Departament o‘ziga yuklangan vazifalar va funksiyalarni bajarish uchun quyidagi huquqlarga ega:

bankning tarkibiy bo‘linmalaridan ish uchun zarur bo‘lgan ma’lumotlarni so‘rash va olish;

bankda axborot va bank xavfsizligini ta’minlash bo‘yicha barcha rejalarni boshqarish;

siyosatni o‘zgartirish bo‘yicha takliflar ishlab chiqish va kiritish;

bankda axborot va bank xavfsizligini ta’minlash bo‘yicha amaldagi me’yoriy-uslubiy hujjatlarni o‘zgartirish va yangilarini qabul qilish;

bank xodimlarini, ularning vazifa va vakolatlarini belgilagan holda, bank rahbariyati bilan kelishilgan holda, axborot va bank xavfsizligini ta’minlash jarayoniga qo‘shimcha ravishda jalb etish;

axborotni texnik va kriptografik himoya qilish talablariga, shuningdek bank xavfsizligini ta’minlash talablariga muvofiqligini tekshirish;

bank xodimlari, birinchi navbatda, maksimal vakolatlarga ega bo'lgan xodimlarning axborot xavfsizligi talablariga rioya etilishini nazorat qilish;

bank xodimlaridan axborotni qayta ishlash texnologiyalarini qo‘llash hamda axborot resurslari va tizimlarining ishlashi to‘g‘risidagi ma’lumotlarni, shuningdek o‘z xizmat vazifalari doirasida boshqa ma’lumotlarni olish;

texnik topshiriqlarni va axborot tizimlarini, shuningdek bankning boshqa obyektlarini yaratish va rivojlantirish loyihalarini ko‘rib chiqish hamda ularga

axborot va bank xavfsizligini ta’minlash nuqtai nazaridan takliflar kiritish;

axborot tizimlarida axborot xavfsizligi tizimini ishlab chiqish, sinovdan o‘tkazish va qabul qilishda ishtirok etish, ushbu jarayonlarda bank ma’lumotlari va boshqa konfidensial ma’lumotlarning chiqib ketishining oldini olish bo‘yicha amaliy choralar ko‘rish;

o'z vakolatlari doirasida bankning axborot va bank xavfsizligini boshqarish, ta'minlash va nazorat qilish usullari, vositalari va mexanizmlarini tanlash, amalga oshirish va qo'llash;

bank bino va xonalarida jismoniy va yong‘in xavfsizligini ta’minlovchi texnik vositalar bilan jihozlash bo‘yicha rahbariyatga ularni yaxshilash bo‘yicha takliflar kiritish;

bank xodimlaridan kirish nazorati va obyekt ichidagi rejimning buzilishi faktlari, shuningdek, axborot xavfsizligi talablari bo'yicha yozma tushuntirishlarni so'rash;

bank obyektlarida qo'riqlash va yong'in signalizatsiyasining texnik vositalarining mavjudligi, holati va ishlashini tekshirish;

bank rahbariyatiga xavfsizlikni takomillashtirish va kuchaytirish yuzasidan takliflar kiritish, kamchiliklar aniqlangan taqdirda bank rahbariyati bilan kelishilgan holda ularni bartaraf etish choralarini ko‘rish;

bank xodimlarining axborot va bank xavfsizligi talablarini bajarishini nazorat qilish;

o'z vakolatlari doirasida bankning axborot va bank xavfsizligini ta'minlash usullari, vositalari va mexanizmlarini tanlash, amalga oshirish va qo'llash;

axborot va bank xavfsizligini ta'minlash bilan bog'liq materiallar va ishlarni qabul qilishda komissiyalar a'zosi sifatida ishtirok etish;

axborot va bank xavfsizligining buzilishi bilan bog‘liq hodisalarni ichki tekshirishni tashkil etish, axborot va bank xavfsizligini ta’minlash talablarini buzganlikda aybdor shaxslarni javobgarlikka tortish bo‘yicha rahbariyatga takliflar kiritish.

V. Javobgarligi

22. Departament direktori va xodimlari quyidagilar uchun javobgardirlar:

ushbu nizom bo'yicha o'z majburiyatlarini bajarmaslik yoki lozim darajada bajarmaslik;

bankda axborot va bank xavfsizligini ta’minlash bo‘yicha ularning ish sifati;

bank tarmoqlari, axborot resurslari va tizimlari, shuningdek, jismoniy obyektlari va moddiy boyliklarini muhofaza qilishning belgilangan darajasini holati va ta’minlash.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
5-ilova

Bank xizmatlari markazlarida Xavfsizlik va axborotni muhofaza qilish bo’limi to‘g‘risidagi namunaviy nizom

I. Umumiy qoidalar

1. Mazkur nizom “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – bank) bank xizmatlari markazlarida (keyingi o‘rinlarda - BXO) Xavfsizlik va axborotni himoya qilish bo’limining (keyingi o‘rinlarda - bo’lim deb yuritiladi) vakolatlari, vazifalari, huquq va majburiyatlarini belgilash maqsadida ishlab chiqilgan.

2. Bo’limning asosiy faoliyati MBXO va unga qarashli bank xizmatlari markazlari (keyingi o'rinlarda BXM deb yuritiladi), masofaviy kassalarning barqaror ishlashini ta'minlash va xavfsizlik tahdidlarni oldini olishdan iborat.

3. Bo‘lim MBXOning mustaqil tarkibiy bo‘linmasi hisoblanadi.

4. Bo'lim MBXO boshlig'iga hisobot beradi.

5. Bo’lim faoliyatini uning boshlig'i boshqaradi, u bevosita BXM rahbariga bo'ysunadi. axborot va bank xavfsizligini ta’minlash masalalari bo‘yicha bo’lim bank Xavfsizlik va axborotlarni muhofaza qilish departamentiga hisobot beradi.

6. Bo’lim boshlig‘i va xodimlari O‘zbekiston Respublikasi qonunchiligiga muvofiq bank Xavfsizlik va axborotlarni muhofaza qilish departamenti bilan kelishilgan holda MBXO rahbarining buyrug’i bilan ishga qabul qilinadi va lavozimidan ozod etiladi.

7. Bo’limning tuzilmasi va shtat jadvali faoliyat shartlari va xususiyatlaridan, shuningdek, bajarilgan ishlar hajmidan kelib chiqqan holda bank boshqaruvi Raisi tomonidan tasdiqlanadi.

8. Bo’lim xodimlarining vazifalari, huquq va majburiyatlari tasdiqlangan namunaviy lavozim yo‘riqnomalari bilan tartibga solinadi.

9. Bo‘limning shtatdagi lavozimlariga shaxsiy va ishbilarmonlik fazilatlari, kasbiy mahorati va sog‘lig‘i holatiga ko‘ra o‘z lavozimida xizmat vazifalarini bajarishga qodir bo‘lgan oliy, asosan texnik ma’lumotga ega bo‘lgan shaxslar qabul qilinadi.

10. Bo'lim xodimi ishda bo'lmagan davrda (ta'til, kasallik, xizmat safari va boshqalar) uning vazifalari bo'lim boshlig'ining qarori bilan vaqtincha uning o'rnini bosuvchi boshqa xodimga yuklanadi.

11. Bo'lim xodimlari o'z faoliyatida quyidagilarga rahbarlik qiladilar:

bankning axborot xavfsizligi siyosati;

axborot xavfsizligi sohasidagi normativ-huquqiy dalolatnomalar va normativ hujjatlar;

MBXO va bank buyruqlari va ko'rsatmalari;

qonun hujjatlari, ichki mehnat qoidalari.

II. Asosiy vazifalari

12. Axborot xavfsizligini ta’minlash bo‘yicha bo’limning asosiy vazifalari quyidagilardan iborat:

1) MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda axborot xavfsizligini ta'minlash va axborot xavfsizligi holatini nazorat qilish bo'yicha chora-tadbirlarni amalga oshirish;

2) MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda axborot xavfsizligi hodisalariga javob berish;

3) konsalting va uslubiy yordam ko'rsatish va MBXO va unga bo'ysunuvchi BXM, masofaviy kassalar xodimlari tomonidan axborot xavfsizligi talablariga rioya etilishini nazorat qilish.

13. Moddiy resurslar va boyliklarning yaxlitligi va xavfsizligini ta'minlash nuqtai nazaridan, MBXO va unga bo'ysunuvchi BXM, masofaviy boshqaruv tizimida obyektlarga xavfsiz jismoniy kirish rejimi, shuningdek yong'in xavfsizligi (keyingi o'rinlarda - bank xavfsizligi deb yuritiladi). Kassalar bo'limining asosiy vazifalari quyidagilardan iborat:

1) MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda bank xavfsizligini ta'minlash choralarini ko'rish va bank xavfsizligi talablariga rioya etilishini nazorat qilish;

2) favqulodda vaziyatlarning oldini olish va bartaraf etish, xodimlarning xavfsizligini ta'minlash va ular MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda yuzaga kelgan zararni kamaytirish bo'yicha ishlarni tashkil etish va amalga oshirish.

III. Vazifalar

14. Axborot xavfsizligini ta'minlash bo'yicha bo’limning vazifalariga quyidagilar kiradi:

1) chora-tadbirlarni amalga oshirish va axborot xavfsizligi holatini nazorat qilish:

bank Xavfsizlik va axborotlarni muhofaza qilish departamentiga MBXO va uning tasarrufidagi BXM, masofaviy kassalarda axborot xavfsizligi tizimini takomillashtirish bo‘yicha takliflar kiritish;

tasdiqlangan rejalarga muvofiq MBXOda axborot xavfsizligini ta'minlash bo'yicha chora-tadbirlarni amalga oshirish;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda axborot xavfsizligi tizimini joriy etish, rivojlantirish va qo'llab-quvvatlash;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda, shu jumladan virusga qarshi himoya vositalarida axborot xavfsizligi vositalarining ishlashi va sozligini nazorat qilish;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda axborot xavfsizligini ta'minlashning ishtiroki va auditini o'tkazish, axborot xavfsizligi talablariga nomuvofiqliklarni, zaifliklarni va ma'lumotlarning chiqib ketish kanallarini aniqlash;

faoliyat yuritish va xavfsizlikni ta'minlashdagi kamchiliklarni aniqlash,

ularni bartaraf etish bo'yicha takliflar kiritish yoki choralar ko'rish;

axborot xavfsizligini ta'minlash holatini monitoring qilish va ko'rilgan choralar hamda MBXO da qo'llaniladigan axborotni himoya qilish vositalarining samaradorligini baholash;

bank Xavfsizlik va axborotlarni muhofaza qilish departamenti bilan MBXOda axborot xavfsizligini ta'minlash bo'yicha kelishilgan harakatlarni ta'minlash bo'yicha o'zaro hamkorlik;

MBXOda konfidensial ma'lumotlarni saqlash hamda uzatish uchun foydalaniladigan ma'lumot saqlovchi va tashuvchi qurilmalar, elektron raqamli imzo kriptografik kalitlarining (keyingi o'rinlarda ERI deb yuritiladi) himoyalangan USB-tashuvchilari hisobini yuritish;

2) Axborot xavfsizligi hodisalariga javob choralari:

bank Xavfsizlik va axborotlarni muhofaza qilish departamentini va bank ATB MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda sodir bo'lgan noxush holatlar to'g'risida monitoring qilish, aniqlash va o'z vaqtida xabardor qilish;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda sodir bo'lgan hodisalarni tahlil qilishda ishtirok etish va ular bo'yicha tekshiruvlar o'tkazish;

axborot xavfsizligi hodisalarining oqibatlarini bartaraf etish va MBXO va unga bo'ysunuvchi BXM, masofaviy kassalar faoliyatini tiklash bo'yicha chora-tadbirlarda ishtirok etish.

3) maslahat va uslubiy yordam ko'rsatish va xodimlar tomonidan axborot xavfsizligi talablariga rioya etilishini nazorat qilish:

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalar xodimlarini siyosat bilan tanishtirish va ularga axborotni himoya qilish bo'yicha ichki me'yoriy hujjatlar talablarini yetkazish;

tarmoq xodimlari tomonidan siyosat qoidalari va talablarining bajarilishini, shuningdek, ularning axborot xavfsizligini ta'minlash bo'yicha tashkiliy-ma'muriy hujjatlar talablariga rioya etilishini nazorat qilish;

bank axborot xavfsizligi siyosati talablarini bajarish bo'yicha brifing, bilim va amaliy ko'nikmalarni MBXO va unga qarashli BXM, masofaviy kassalar xodimlari tomonidan baholash.

15. Bo'limning bank xavfsizligini ta'minlash bo'yicha vazifalariga quyidagilar kiradi:

1) chora-tadbirlarni amalga oshirish va bank xavfsizligi talablariga rioya etilishini nazorat qilish:

MBXO va uning tasarrufidagi BXM, masofaviy kassalarda bank xavfsizligini ta'minlashda mavjud kamchilik va huquqbuzarliklarni bartaraf etish yuzasidan takliflar ishlab chiqish va rahbariyatga kiritish;

MBXO va BXM hududi va xonalariga kirishda xavfsizlik va kirishni nazorat qilishni tashkil etish;

kirishni cheklash rejimiga rioya etilishi ustidan nazoratni amalga oshirish va taqiqlangan hududlarga, shu jumladan himoya qilinadigan xonalarga ruxsatsiz kirishga urinishlarning oldini olish;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda qo'riqlash, signalizatsiya va yong'in signalizatsiyasi, ogohlantirish tizimlari, yong'in o'chirish,

videokuzatuv, kirishni boshqarish va (SKUD) boshqarish uskunalarini, ulardan foydalanish, texnik xizmat ko'rsatish va ta'mirlashni tashkil etish;

MBXOda loyihalash, o'rnatish va ishga tushirish bosqichlarida texnik xavfsizlik tizimlari bilan jihozlash bo'yicha ishlarni pudratchilar va subpudratchilar tomonidan bajarilishi ustidan nazoratni amalga oshirish;

nazorat-kassa mashinalarining jihozlanishini ularning qurilmasiga va texnik mustahkamligiga qo'yiladigan talablarga muvofiq nazorat qilish;

MBXO xodimlari tomonidan MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda sanitariya me'yorlari, yong'in va xavfsizlik talablariga rioya etilishi ustidan nazoratni amalga oshirish;

MBXO va unga bo'ysunuvchi BXMda, masofaviy kassalarda videokuzatuv tizimlari, xavfsizlik va yong'in signalizatsiya tizimlari, yong'in o'chirish tizimlarini tashkil etish talablariga rioya qilish bo'yicha tekshiruvlarda ishtirok etish.

2) favqulodda vaziyatlarning oldini olish va ularni tugatish:

favqulodda vaziyatlar sodir bo'lgan taqdirda chora-tadbirlarni tashkil etish, amalga oshirish tartibi, usullari va muddatlarini, shuningdek davlatning barcha darajalarida o'zaro hamkorlik rejasini belgilaydigan MBXO va uning xodimlarining fuqarolik muhofazasi obyektida favqulodda vaziyatlarda profilaktika va harakat qilish tizimi rejasini ishlab chiqish;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda favqulodda vaziyatlarning oldini olish va bartaraf etish bo'yicha chora-tadbirlarni amalga oshirish;

favqulodda vaziyat yoki yong'in sodir bo'lgan taqdirda xodimlarni va moddiy boyliklarni evakuatsiya qilishga tayyorgarlik ko'rish va o'tkazishni rejalashtirish;

MBXOda favqulodda vaziyatlarni bartaraf etish uchun moliyaviy va moddiy resurslar zaxirasini shakllantirish bo'yicha ishlarda ishtirok etish;

favqulodda vaziyatlarda MBXO xodimlarining hayotini ustuvor ta'minlash bo'yicha favqulodda qutqaruv va boshqa ishlarda ishtirok etish.

IV. Huquqlari

16. Bo‘lim o‘ziga yuklangan vazifalar va funksiyalarni bajarish uchun quyidagi huquqlarga ega:

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda himoya tizimini takomillashtirish bo'yicha takliflar kiritish;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalar xodimlarining faoliyatini nazorat qilish, ulardan axborot va bank xavfsizligini ta'minlash masalalari bo'yicha ma'lumot olish;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalardagi nosozliklar va baxtsiz hodisalardan keyin ish faoliyatini tiklash bo'yicha tadbirlarda ishtirok etish;

bo’lim xodimlarining malaka darajasini oshirish bo’yicha taklif kiritish va bank mablag‘lari hisobidan malaka oshirish;

MBXO rahbariyatiga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga MBXO va unga qarashli BXMlarni, masofaviy kassalarni bank xavfsizligini ta’minlashning texnik vositalari bilan jihozlash bo‘yicha takliflar,

shuningdek ularni takomillashtirish bo‘yicha takliflar kiritish;

MBXO xodimlarining axborot va bank xavfsizligi talablarini bajarishini nazorat qilish.

V. Javobgarligi

17. Bo'lim boshlig'i va xodimlari quyidagilar uchun javobgardirlar:

ushbu nizom bo'yicha o'z majburiyatlarini bajarmaslik yoki lozim darajada bajarmaslik;

MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda axborot va bank xavfsizligini ta'minlash bo'yicha ularning ish sifati;

MBXO tarmoqlari, axborot resurslari va tizimlarini, shuningdek, MBXO va unga bo'ysunuvchi BXMning jismoniy obyektlari va moddiy boyliklarini, masofaviy kassalarni himoya qilishning belgilangan darajasini holati va ta'minlash.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
6-ilova

Tizimli va amaliy dasturlarni yangilash, shuningdek ma’lumotlarni zaxira nusxalarini shakllantirish va tiklash to‘g‘risidagi nizom

I. Umumiy qoidalar

1. “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank)ning tizimli va amaliy dasturiy ta’minotni yangilash, shuningdek ma’lumotlarni zaxiralash va tiklash to‘g‘risidagi ushbu nizom quyidagilarni belgilaydi:

tizim va amaliy dasturiy ta'minotni yangilash, ularga o'zgartirish va qo'shimchalar kiritish tartibi;

uskunalarning ishlamay qolishi, axborot xavfsizligi buzilishi, foydalanuvchilarning xatolari, favqulodda vaziyatlar (yong‘in, tabiiy ofatlar va boshqalar) natijasida to‘liq yoki qisman yo‘qolgan axborot tizimlari yoki ularning qismlarining ishini keyinchalik tiklash uchun ma’lumotlarni zaxira qilish tartibi;

ma'lumotlarni zaxiralash va dasturiy ta'minotni yangilash bilan shug'ullanadigan shaxslarning javobgarligi.

2. Ushbu nizom quyidagi faoliyat turlarini tartibga soladi:

zaxira nusxalash;

zaxira nusxalashning nazorati;

zaxira nusxalarini saqlash;

dasturiy ta’minotni yangilash va o’zgartirish kiritish.

3. Zaxiralashning maqsadi - apparat, dasturiy ta’minot ishdan chiqqanda yoki favqulodda vaziyatlar yuzaga kelganda ma’lumotlarning yo‘qolishini oldini olish.

4. Ushbu nizom tizim va amaliy dasturiy ta’minotga nisbatan, shuningdek - bankning axborot tizimlarida foydalaniladigan ma’lumotlarga qo‘llaniladi.

II. Atamalar, ta'riflar va qisqartmalar

5. Ushbu nizomda quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

1) **zaxiralash:** ma'lumotlar tashuvchida (qattiq disk, floppi va boshqalar) nusxasini yaratish jarayoni, shikastlangan yoki yo'q qilingan taqdirda ma'lumotlarni asl yoki yangi joyiga qaytarish uchun mo'ljallangan;

2) **server:** Kompyuterning boshqa kompyuterga xizmat ko'rsatishiga imkon beruvchi apparat va dasturiy ta'minot (server dasturiy ta'minoti) to'plami. Kompyuterlar server dasturi bilan mijoz dasturlari yordamida ishlaydi.

III. Dasturlarni o‘rnatish, o‘zgartirishlar kiritish, sozlash va yangilash vazifalari

6. Dasturiy ta'minotni o'rnatish, o'zgartirish, sozlash va dasturiy ta'minotni

yangilash vazifalariga quyidagilar kiradi:

yangi ishlab chiqilgan, o'zgartirilgan yoki sotib olingan dasturiy ta'minotni o'rnatish;

dasturiy ta'minotni sozlash (konfiguratsiya);

dasturiy ta'minotni sozlash (konfiguratsiya)ga o'zgartirishlar kiritish;

dastur yoki axborot tizimining ayrim vazifalari va funksiyalarini o'zgartirish zarurati tug'ilganda dasturiy ta'minotning dastlabki kodiga o'zgartirishlar kiritish;

yangi ishlab chiqilgan dasturiy ta'minotni yoki o'zgartirilgan dasturiy ta'minotni mavjud uskunaga o'rnatishdan oldin sinovdan o'tkazish (ishga tushirish);

ishlab chiqaruvchilardan (ishlab chiquvchilardan) dasturiy ta'minot yangilanishlarini kuzatish;

dasturiy ta'minotni yangilash;

dasturiy ta'minotni o'rnatish va sozlash, sozlamalarga o'zgartirishlar kiritish va dasturiy ta'minotni yangilashdan keyin uning to'g'ri ishlashini tekshirish.

7. O'zgartirishlar kiritish, dasturiy ta'minotni sozlash va yangilash vazifalari quyidagilarga yuklangan:

korporativ tarmoq administratori va Axborot texnologiyalari departamentining Telekommunikatsiya va aloqa bo‘limi - korporativ tarmoqning tarmoq jihozlari;

bank Axborot texnologiyalari departamentining Active Directory tizimi administratori va Telekommunikatsiyalar va aloqa bo‘limi - Bosh ofis AB domen kontrolleri va fayl serveri serverlarining operatsion tizimi;

Axborot texnologiyalari departamentining AT infratuzilmasini rivojlantirish va qo‘llab-quvvatlash boshqarmasi xodimlari - korporativ elektron pochta tizimi uchun dasturiy ta’minot, IP telefoniya va videokonferensiya aloqa tizimlari, Bosh ofis AB ish stansiyalari uchun operatsion tizimlar;

axborot tizimlari administratorlari, Dasturlash boshqarmasi va jarayonlarni ishlab chiqish va qo'llab-quvvatlash boshqarmasi - bank (ABT, Internet-Banking, mobil Banking) axborot tizimlarining operatsion tizimlari va ma'lumotlar bazasi serverlarining ma'lumotlar bazasi serverlarining amaliy tizimlari va ilovalari serverlari, CRM tizimlari, korporativ ma'lumotlarni saqlash DWH, CROBS tizimlari, ELMA BPM tizimlari, EHAT tizimlari, SAP tizimlari, Way4 tizimlari va boshqalar);

Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotni himoyasi qilish boshqarmasi xodimlari - axborot xavfsizligini ta’minlash bo‘yicha dasturiy ta’minot (tarmoqlararo ekran, IDPS vositalari, DLP tizimi, PAM tizimi, virusga qarshi himoya tizimi, axborot xavfsizligi monitoringi va hodisalarni boshqarish tizimlari, ERI kalitlarini ro‘yxatga olish markazi va boshqalar);

MBXO Axborot texnologiyalari bo'limi xodimlari - MBXO va BXM fayl serverining operatsion tizimlari, MBXO, BXMdagi ish stansiyalari, masofaviy kassalar.

8. Quyidagi hollarda dasturiy ta'minot o'rnatish amalga oshiriladi:

axborot tizimi yoki vositalarini ishga tushirishda;

bank tarkibiy bo‘linmalarining arizasi asosida;

almashtirish, yangisini o'rnatish yoki mavjud qurilmani qayta o'rnatishda.

9. O'zgartirishlar va dasturiy ta'minotni yangilash quyidagi hollarda amalga

oshiriladi:

dasturiy ta'minot ishlab chiqaruvchisi (ishlab chiqaruvchisi) tomonidan yangi versiya yoki yangilanishlarning paydo bo'lishi;

dasturiy ta'minotda aniqlangan zaifliklar yoki xatolarni bartaraf etish ehtiyojlari;

dasturiy ta'minotning vazifalari va funksiyalaridagi o'zgarishlar ehtiyojlari.

10. Dasturiy ta'minotga kiritilgan barcha o'zgartirishlar va yangilanishlar ushbu nizomning 7-bandida ko'rsatilgan mas'ul xodimlar tomonidan qat'iy nazorat qilinishi kerak. Har bir amaliyot uchun test protseduralari tayyorlanadi.

11. Ishlab chiqaruvchi yoki yaratuvchi muhim yoki asosiy deb baholagan dasturiy ta'minotga o'zgartirishlar va yangilanishlar uchun qo'llash tartibini boshlash. Muhim va asosiy sozlashlarni yoki yangilanishlarni qo‘llash zarurati to‘g‘risidagi qarorlar Axborot texnologiyalari departamenti direktori yoki Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori tomonidan bildirishnoma olingan kundan boshlab 3 (uch) kun ichida qabul qilinadi. Bunday yangilanishlarni o'rnatish rad etilgan taqdirda, rad etilgan yangilanish bilan bartaraf etilgan aniqlangan zaifliklar yoki xatolarni bartaraf etish uchun tegishli choralar ko'rish kerak.

12. Dasturiy ta'minot va tizim dasturiy ta'minoti uchun yangilanishlarning chiqarilishi haqidagi ma'lumot manbai dasturiy ta'minot ishlab chiqaruvchisi, ixtisoslashgan Internet saytlari va boshqalarning pochta ro'yxatlari bo'lishi mumkin. Yo'qolgan yangilanishlar haqidagi ma'lumotlarning yana bir manbai zaifliklarni aniqlash va boshqarish tizimi natijalari, xavfsizlik skanerlari natijalar bo'lishi mumkin.

13. Quyidagi dasturiy ta'minot majburiy yangilanishi kerak:

domen kontrolleri serverining operatsion tizimlari, ma'lumotlar bazasi serverlari va axborot tizimlarini qo'llash serverlari, ERI kalitlarini ro'yxatga olish markazi serveri, korporativ elektron pochta serveri va boshqa axborot almashish tizimlari;

bank axborot tizimlari ma'lumotlar bazasi serverlarining ma'lumotlar bazasi;

bank axborot tizimlari dastur serverlarining ilovalari;

axborot xavfsizligi vositalarining dasturiy ta'minoti va xavfsizlik vositalari serverlarining operatsion tizimi.

Bank barcha tarkibiy bo‘linmalari xodimlarining ish joylarida o‘rnatilgan operatsion tizimlar WSUS yangilash serveri orqali yangilanadi.

14. 13-bandda ko'rsatilgan dasturiy ta'minotni yangilash zarurligi to'g'risidagi qaror Axborot texnologiyalari departamenti direktori va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktorining qarori bilan qabul qilinadi. Ushbu yangilanishlar kerak bo'lganda serverlar va jihozlarni yuqori hajmni hisobga olgan holda ishlamaydigan vaqtlarda amalga oshirilishi kerak. Yangilashdan so'ng serverlar va uskunalarning normal ishlashini, yangilangan dasturiy ta'minotni, ularga o'rnatilgan amaliy dasturiy ta'minotni va ma'lumotlarning xavfsizligini baholash uchun barcha tekshiruvlar va testlar o'tkazilishi kerak. Yangilangan dasturiy ta'minot yoki dasturiy ta'minot sozlamalari kerak bo'lganda zaxiralanadi.

15. Amaliy dasturiy ta’minotga o‘zgartirishlar uni ishlab chiquvchi tomonidan o‘zgartirilgan taqdirda, bankning funksional imkoniyatlariga yoki

axborot tizimlarini yanada rivojlantirishga o‘zgartirishlar kiritish zarurati tug‘ilganda amalga oshiriladi.

ABT va boshqa axborot tizimlari uchun ularning amaliy dasturlarini modifikatsiya va o'zgartirish uchun quyidagi talablar bajarilishi kerak:

modifikatsiya yoki o'zgartirilgan amaliy dasturiy ta'minot axborot tizimining barcha mavjud va yangi funksiyalari ishlashini tekshirish bilan alohida test serverlarida sinovdan o'tkazilishi kerak;

tasdiqlangan modifikatsiya yoki o'zgartirilgan amaliy dasturiy ta'minotni to'liq tekshirilgandan keyin ish soatlaridan keyin o'rnatish;

modifikatsiya yoki o'zgartirilgan amaliy dasturlarni o'rnatishda axborot tizimining ma'lumotlar bazasidagi barcha ma'lumotlarning saqlanishini ta'minlash;

o'rnatilgandan so'ng serverlarning normal ishlashini, ularga o'rnatilgan modifikatsiya yoki o'zgartirilgan amaliy dasturiy ta'minotni va axborot tizimi ma'lumotlarining xavfsizligini baholash uchun barcha tekshiruvlar va testlarni o'tkazish.

IV. Tizim va amaliy dasturiy ta’minotni yangilash uchun javobgarlik

16. Tizim va amaliy dasturiy ta'minotni yangilash uchun javobgarlik ushbu nizomning 7-bandida ko'rsatilgan xodimlar zimmasiga yuklanadi.

17. Xizmat xodimlari tomonidan tizim va amaliy dasturlarni yangilash talablariga rioya etilishini nazorat qilish Axborot texnologiyalari departamenti hamda Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan amalga oshiriladi.

V. Zaxira turlarining tasnifi

18. Turlarga ko‘ra zaxira qilingan ma’lumotlar quyidagilarga bo‘linadi:

operatsion tizimlar va yordamchi dasturlar;

amaliy (ixtisoslashtirilgan) dasturiy ta’minot;

ma’lumotlar.

19. Zaxira ma'lumotlarini saqlash joylari:

serverlar;

ishchi stansiyalar;

bo'sh qattiq disklar yoki ma'lumotlarni saqlash tizimlarining qattiq disklarida bo'sh joy;

olinadigan vositalar (magnit lentalar, DVD disklar, tashqi qattiq disklar).

20. klonlash (point-in-time), ya’ni jildlarning (klonlarning) bir nechta fizik nusxalarini yaratish;

tezkor nusxani yaratish (snapshot), ya’ni diskning mantiqiy nusxasini, uning obrazini yaratish;

nusxalash.

saqlangan ma’lumotlarning to‘liqligi bo‘yicha:

to‘liq zaxira (Full backup) - barcha ma’lumotlarni zaxira nusxasini yaratish, texnologik uskunalarni to‘liq tiklash uchun zarur;

qo‘shimcha zaxira – (Incremental backup) avvalgi to‘liq yoki qo‘shimcha

zaxiralashdan keyin o‘zgartirilgan barcha ma’lumotlarning zaxira nusxasini yaratish;

differensial zaxiradan farqli o’laroq o’zgargan yoki yangi fayllar eskilarini almashtirmaydi va mustaqil xotiraga yoziladi.

differensial zaxira – (Differential backup) avvalgi to‘liq zaxiralashdan keyin o‘zgartirilgan barcha ma’lumotlarning zaxira nusxasini yaratish.

21. Tashuvchiga kirish usuliga ko‘ra:

onlayn zaxira (Online backup) - doimiy ulangan (to‘g‘ridan-to‘g‘ri yoki tarmoq orqali) zaxira arxivini yaratish;

avtonom zaxira – (Offline backup) foydalanishdan oldin o‘rnatilishi kerak bo‘lgan zaxira nusxasini olinadigan muhitda yoki kartridjda saqlash.

22. Zaxira vaqti bo‘yicha:

real vaqtda zaxira nusxalari - ma’lumotlar tizimda paydo bo‘lganda to‘g‘ridan-to‘g‘ri zaxiralash - ko‘paytirish, tarqatish va hokazo.

rejalashtirilgan zaxira nusxalari - ma’lumotlar oldindan belgilangan vaqtlarda zaxiralanadi.

VI. Zaxira nusxa olish va qayta tiklash tartibi

23. Bank tomonidan to‘lov va boshqa axborot tizimlarining ma’lumotlar bazalari va ularga kiritilgan o‘zgartirishlar majburiy zaxiraga olinishi shart. Tizimning ishlashi va tiklash uchun zarur bo'lgan dasturiy ta'minot va apparat konfiguratsiyalari ham saqlanishi kerak.

24. Ma'lumotlarning zaxira nusxasi quyidagi ma'lumotlar asosida amalga oshiriladi: nusxa ko'chirilgan ma'lumotlarning tarkibi va hajmi, zaxira nusxalarini yaratish chastotasi va nusxalarni saqlash muddati.

25. Zaxira tizimi muhim ma'lumotlarni saqlash uchun yetarli darajada ishlashni ta'minlashi kerak.

Inson omilini bartaraf etish va noto'g'ri ma'lumotlarni qayta tiklash bilan bog'liq zararni minimallashtirish uchun nazorat xodimlarining minimal aralashuvini hisobga olgan holda zaxira va tiklash tizimini avtomatlashtirish kerak.

26. Ma'lumotlarning zaxira nusxasini yaratish, qayta tiklash va arxiv saqlanishini ta'minlash uchun Axborot texnologiyalari departamenti hamda Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimlari orasidan zaxira nusxasini yaratish uchun mas'ullar tayinlanadi.

27. Zaxira nusxalarini olishga mas’ul shaxslar quyidagilarni ta'minlashi kerak:

zaxira tizimini dastlabki sozlash (jadvallar, bildirishnomalar va boshqalarni yaratish), zaxira tizimini ishga tushirish;

zaxira tizimining konfiguratsiyasiga o'zgartirishlar kiritish;

zaxira tizimini ishlatish va texnik xizmat ko'rsatish;

zaxira nusxalarini o'z vaqtida yaratish;

zaxira jurnalini tahlil qilish, zaxira sozlamalarini o'zgartirish zarurligini kuzatish;

nusxalash yoki zaxira uskunalarni nazorat qilish;

zaxira natijalarini nazorat qilish;

zaxira nusxalarini o'z ichiga olgan axborot vositalarini saqlash tartibi va shartlariga, shuningdek, zaxira nusxalarining yaxlitligi va xavfsizligiga rioya qilish;

zaxira nusxasini yaratishda aniqlangan xatolar va nosozliklar to'g'risida rahbariyatga hisobot berish, shuningdek ularni bartaraf etish bo'yicha zarur choralarni ko'rish;

zaxira nusxalaridan ma'lumotlarni tiklash.

28. ABT uchun elektron arxiv O‘zbekiston Respublikasi Markaziy bankining 2020 yil 25 yanvardagi 2/4-son qarori bilan tasdiqlangan O‘zbekiston Respublikasi tijorat Banklarining avtomatlashtirilgan tizimlarida axborotni himoya qilish to‘g‘risidagi nizom talablariga muvofiq yaratilishi kerak.

VII. Zaxira nusxalanadigan ma’lumotlar ro‘yxati

29. Axborot tizimlarining, operatsion tizimlarning, amaliy dasturlarning, tizim konfiguratsiyasining sozligini tiklash uchun zarur bo'lgan ma'lumotlar zaxira qilinishi kerak.

Bank tomonidan zaxira qilinishi kerak bo‘lgan ma’lumotlar ro‘yxati, shuningdek, zaxira nusxasini yaratish uchun mas’ul shaxslar jadvalda keltirilgan.

30. Zaxira qilingan ma'lumotlar ro'yxati yangi axborot tizimlari va vositalari paydo bo'lishi bilan o'zgartirilishi va to'ldirilishi mumkin. Mazkur ro‘yxatga o‘zgartirish va qo‘shimchalar Axborot texnologiyalari departamenti hamda Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan kiritiladi.

31. Favqulodda vaziyat va zaxira tizimi ishlamay qolgan taqdirda, jadvalda ko'rsatilgan axborot tizimlarining ma'lumotlarini zaxiralash qo'lda amalga oshirilishi kerak.

Qo'lda nusxa ko'chirish har kuni ish kunining oxirida server fayl tizimlari vositalaridan foydalangan holda amalga oshiriladi va zaxira nusxasini saqlash uchun kerakli disk maydoni bo'lgan ma'lumotlarni saqlash tizimida saqlanadi.

32. Bundan tashqari, alohida axborot resurslari elektron arxivga joylashtiriladi. Elektron arxiv quyidagi axborot resurslarini o'z ichiga olishi kerak:

bank amaliyoti kunining to'liq elektron ma'lumotlar bazasi;

amal qilish muddati o‘tgan ochiq kalitlar va ERI kalitlari;

kundalik bank amaliyoti dasturlari va alohida Bankda foydalaniladigan boshqa dasturlar majmui;

elektron to'lov tizimlari, dasturiy ta'minot va apparat-dasturiy ta'minot tarmog'i qurilmalari, shuningdek, axborot xavfsizligi hodisalari bilan bog'liq elektron protokollar;

elektron pochta orqali qabul qilingan va yuborilgan to'lovlar bilan bog'liq hujjatlar (buyruqlar, qarorlar va boshqalar);

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

tijorat Banklarining kredit va boshqa bank operatsiyalari to'g'risidagi ma'lumotlari;

bank boshqaruv tizimi haqida ma'lumot.

33. ABT va axborot tizimlaridagi elektron arxivlar tashqi saqlaydigan vositalardan olinadigan tashuvchilarga yozilishi kerak: magnit lentalar, tashqi qattiq disklar, DVD disklar va boshqalar.

34. Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimlaridan tashqi tashuvchilarda qayd etilgan elektron arxivlarning saqlanishi uchun mas'ul shaxs tayinlanadi.

35. Aniqlangan zaxira ma'lumotlarga ruxsatsiz kirishga urinishlar, shuningdek elektron arxivlarning tashqi tashuvchilari o'g'irlanishi va yo'qolishi, zaxiralash jarayonida sodir bo'lgan axborot xavfsizligining boshqa buzilishi holatlari to'g'risida Xavfsizlik va axborotlarni muhofaza qilish departamentiga xabar berish kerak.

1-jadval. “O‘zsanoatqurilishbank” ATBda zaxiralanadigan ma’lumotlari ro‘yxati

№	Zaxira qilinadigan ma’lumotlar	Zaxira olish usuli	Zaxira nusxalash davriyligi	Javobgar
1.	**Bankning avtomatlashtirilgan bank tizimi (ABT)**			
1.1.	ABT ma'lumotlar bazasi, jurnallar	**Zaxiralash uchun** asosiy ma'lumotlarni qayta ishlash markazida asosiy va zaxira ma'lumotlar bazasi serverida RAID saqlash tizimidan foydalanadi (klasterda ishlaydigan jismoniy jihatdan alohida ma'lumotlar bazasi serverlari). **Arxivlash uchun** ma'lumotlar, ma'lumotlarni asosiy server ma'lumotlar bazasidan zaxira ma'lumotlar markazidagi uchinchi zaxira serverining ma'lumotlar bazasiga ko'chiriladi - doimiy ma'lumotlar replikatsiyasi (zaxira BackUpDatabase (Full)). **Zaxiralangan ma’lumotlarni saqlash joyi**: asosiy va zaxira ma'lumotlarni qayta ishlash markazlarida ikkita ortiqcha ABT ma'lumotlar bazasi serverlarining qattiq disklari. **Zaxiralash tizimi:** Oracle Data Guard **Zaxiralash turi:** Fullback-up, Online backup, real vaqtda zaxira nusxalari	Ma'lumotlarni replikatsiyasi avtomatik va real vaqtda sodir bo'ladi	ABT administratori, Axborot texnologiyalari departamentining ishlab chiqish va ABT qo'llab-quvvatlash bo'limi
1.2.	ABT elektron arxivi ma’lumotlar bazasi	Elektron arxiv tashqi axborot vositalarida qayd etiladi: lenta kutubxonasi. **Zaxiralash tizimi:** Oracle RMAN **Zaxiralash turi:** Fullback-up va Incremental backup, Online backup, Offline backup, rejalashtirilgan zaxira nusxalari	Haftada bir marta to'liq, boshqa kunlarda bosqichma-bosqich	

1.3.	MBBT Ma'lumotlar bazasi va dastur serverlarining operatsion tizimi	Zaxira ma'lumotlarni qayta ishlash markazida jismoniy alohida ma'lumotlar bazasi serverida operatsion tizimni takrorlash, asosiy ma'lumotlar bazasi serveri bilan klaster rejimida, shuningdek zaxira ma'lumotlarni qayta ishlash markazida jismoniy alohida kutish ma'lumotlar bazasi serverida ishlash.	Boshqa serverlarda takrorlash	
1.4.	ABT ilova serverlarining operatsion tizimi va ilovalari	Asosiy ma'lumotlarni qayta ishlash markazidagi alohida virtual serverlarda operatsion tizim va dasturni takrorlash. Virtual dastur serverining to'liq nusxasi va zaxira ma'lumotlarni qayta ishlash markazida va lenta kutubxonasida saqlash tizimida saqlash. **Zaxira qilingan ma'lumotlarni saqlash joyi**: zaxira ma'lumotlar markazi va lenta kutubxonasi saqlash tizimi **Zaxiralash tizimi:** Veeam Backup **Zaxiralash turi:** Fullback-up va Incremental backup, Online backup, Offline backup, rejalashtirilgan zaxira nusxalari	Haftada bir marta to'liq, boshqa kunlarda bosqichma-bosqich	
2.	**Internet-Banking va mobil Banking tizimlari**			
2.1.	Ma'lumotlar bazasi, operatsion tizim, internet-Banking va mobil Banking web-ilovasi	**Zaxiralash uchun** Internet-Banking va mobil Banking virtual serverlari zaxira qilinadi va to'liq nusxalanadi va zaxira ma'lumotlarni qayta ishlash markazidagi ma'lumotlarni saqlash tizimida saqlanadi. **Zaxiralangan ma'lumotlarni saqlash joyi**: zaxira ma'lumotlarni qayta ishlash markazi saqlash tizimi **Zaxiralash tizimi:** Veeam Backup **Zaxiralash turi:** Fullback-up, Online backup, rejalashtirilgan zaxira nusxalari	Avtomatik ravishda, har kuni kechasi	Axborot texnologiyalari departamentining Raqamli texnologiyalar va masofaviy bank tizimlarini qo‘llab-quvvatlash bo‘limi
3.	**CRM, SWIFT, Way4, DWH, CROBS, SAP axborot tizimlari**			

3.1.	Ma'lumotlar bazasi, operatsion tizim, axborot tizimlari ilovasi	**Zaxiralash uchun** virtual axborot tizimining serverlari zaxira qilinadi va to'liq nusxalanadi va zaxira ma'lumotlarni qayta ishlash markazida saqlash tizimida saqlanadi. **Zaxira qilingan ma'lumotlarni saqlash joyi**: zaxira ma'lumotlarni qayta ishlash markazi saqlash tizimi va Way4 tizimi uchun qo'shimcha ravishda lenta kutubxonasi **Zaxira qilish tizimi:** Oracle RMAN, Veeam Backup **Zaxiralash turi:** Fullback-up, Online backup, rejalashtirilgan zaxira nusxalari	Avtomatik ravishda, har kuni kechasi	Axborot tizimlari 115dministrator, Axborot texnologiyalari departamenti
3.	**ELMA BPM va EHAT axborot tizimlari**			
3.1.	Ma'lumotlar bazasi, operatsion tizim, axborot tizimlari ilovasi	**Zaxira qilish uchun** axborot tizimlarining virtual serverlari to'liq nusxa ko'chiriladi va zaxira ma'lumotlar markazidagi saqlash tizimida saqlanadi. **Zaxiralangan ma'lumotlarni saqlash joyi**: zaxira ma'lumotlarni qayta ishlash markazi saqlash tizimi **Zaxiralash tizimi:** MySQL, Veeam Backup **Zaxiralash turi:** Fullback-up, Online backup, rejalashtirilgan zaxira nusxalari	Avtomatik ravishda, har kuni kechasi	Axborot tizimlari administratori, Axborot texnologiyalari departamenti
4.	**ELMA BPM va EHAT axborot tizimlari**			
4.1.	Ma'lumotlar bazasi, operatsion tizim, axborot tizimlari ilovasi	**Zaxira qilish uchun** axborot tizimlarining virtual serverlari to'liq nusxa ko'chiriladi va zaxira ma'lumotlarni qayta ishlash markazidagi saqlash tizimida saqlanadi **Zaxira qilingan ma'lumotlarni saqlash joyi**: zaxira ma'lumotlarni qayta ishlash markazi saqlash tizimi **Zaxira qilish tizimi:** MySQL, Veeam Backup **Zaxira qilish turi:** Fullback-up, Online backup, rejalashtirilgan zaxira nusxalari	Avtomatik ravishda, har kuni kechasi	Axborot tizimlari administratori, Axborot texnologiyalari departamenti
5.	**Bankning ERI kalitlarini ro'yxatga olish markazi**			

5.1	ERI kalitlarini ro'yxatga olish markazining ma'lumotlar bazasi, jurnallar, operatsion tizim, amaliy dastur	**Zaxiralash uchun** asosiy ma'lumotlarni qayta ishlash markazidagi ERI kalitlarini ro'yxatga olish markazining jismoniy serveri zaxira ma'lumotlarni qayta ishlash markazidagi alohida jismoniy serverga zaxiralanadi va to'liq nusxa ko'chiriladi va zaxiraviy ma'lumotlar markazida va tashqi muhitda ma'lumotlarni saqlash tizimida saqlanadi. **Zaxiralangan ma'lumotlarni saqlash joyi**: zaxira ma'lumotlarni qayta ishlash markazi saqlash tizimi va tashqi tashuvchilar **Zaxiralash tizimi:** Veeam Backup **Zaxiralash turi:** Fullback-up, Online backup, rejalashtirilgan zaxira nusxalari	Avtomatik ravishda, har kuni tunda ERI kalitlarini ro'yxatdan o'tkazish markazining serveri to'liq zaxiralanadi va zaxiraviy ma'lumotlar markazi va tashqi tashuvchilarning ma'lumotlarni saqlash tizimida qayd etiladi.	Axborot tizimlari administratori, Axborot texnologiyalari departamenti
6.	**Bankning korporativ elektron pochtasi va Banklararo elektron pochtasi**			
6.1.	Korporativ va Banklararo elektron pochta serveri ma'lumotlar bazasi, jurnallar, operatsion tizim, ilovalar	**Zaxiralash uchun** asosiy ma'lumotlarni qayta ishlash markazidagi virtual korporativ va Banklararo elektron pochta serverlari to'liq nusxa ko'chiriladi va zaxira ma'lumotlarni qayta ishlash markazida va tashqi tashuvchi ma'lumotlarni saqlash tizimida saqlanadi. **Zaxiralangan ma'lumotlarni saqlash joyi**: zaxira ma'lumotlarni qayta ishlash markazi saqlash tizimi va tashqi tashuvchilar **Zaxiralash tizimi:** Veeam Backup **Zaxiralash turi:** Fullback-up, Online backup, rejalashtirilgan zaxira nusxalari	Avtomatik ravishda, har kuni tunda to'liq korporativ va Banklararo elektron pochta serverining zaxira nusxasi yaratiladi va zaxira ma'lumotlarni qayta ishlash markazi saqlash tizimida va tashqi muhitda tashuvchi vositada qayd etiladi.	Axborot texnologiyalari departamenti
7.	**Bankning rasmiy web-sayti va Internet tarmog‘i hamda Intranet tizimining web-sayti**			
7.1.	Ma'lumotlar bazasi, operatsion tizim web-sayti ilovasi	**Zaxiralash uchun** provayderning xosting platformasidagi rasmiy web-saytning virtual serveri, shuningdek, Intranet tizimining virtual serveri to‘liq nusxalanadi va ma’lumotlarni zaxiralash markazidagi ma’lumotlarni saqlash tizimida saqlanadi..	Qo'lda, har kuni kechasi	Veb-saytlarni ishlab chiqish, Internet va onlayn resurslarni boshqarish guruhi, Axborot

		Zaxiralangan ma'lumotlarni saqlash joyi: zaxira ma'lumotlarni qayta ishlash markazi saqlash tizimi. **Zaxiralash tizimi:** Veeam Backup **Zaxiralash turi:** Fullback-up, Offline backup, rejalashtirilgan zaxira nusxalari		texnologiyalari departamenti
8.	**Tarmoqlararo ekran, marshrutizatorlar, IDPS uskunalari va proksi-server**			
8.1.	Apparat - dasturiy ta'minotning konfiguratsiyasi parametrlari (sozlamalari).	Konfiguratsiya fayllarini alohida tashqi qattiq diskka va administrator ish stansiyasiga nusxalash **Zaxiralash turi:** Incremental backup, Offline backup, rejalashtirilgan zaxira nusxalari	Qo'lda, sozlamalarni o'zgartirganda, shuningdek, dasturiy ta'minotni yangilashdan keyin	Xavfsizlik va axborotlarni muhofaza qilish departamenti Axborot himoyasi boshqarmasi
9.	**Asosiy tarmoq uskunalari, IP-telefoniya va video konferentsiya tizimlari**			
9.1.	Korporativ tarmoq kommutatorlarining konfiguratsiyasi parametrlari (sozlamalari).	Sozlamalar fayllarini alohida tashqi qattiq diskka va administrator ish stansiyasiga nusxalash **Zaxiralash turi:** Incremental backup, Offline backup, rejalashtirilgan zaxira nusxalari	Sozlamalarni o'zgartirish va dasturiy ta'minotni yangilashda qo'lda	korporativ tarmoq administratori, Axborot texnologiyalari departamentining Telekommunikatsiyalar va aloqa bo'limi

VIII. Zaxira nusxasini o‘z ichiga olgan tashuvchi vositalarini saqlash tartibi va shartlari

36. Zaxira nusxasini saqlaydigan ma’lumot tashuvchilarga, ushbu ma’lumotlarning eng yuqori konfidensiallik darajasiga qarab konfidensiallik darajasi belgilanadi.

37. Zaxira nusxalari va elektron arxivlar uchun tashqi tashuvchi vositalar hisobga olinishi va belgilanishi kerak (nusxa olish sanasi, resurs nomi, amal qilish muddati, nusxalar soni, jild raqami va boshqalar).

38. Zaxira nusxalari va elektron arxivlarning tashqi tashuvchilari hisobi Xavfsizlik va axborotlarni muhofaza qilish departamentining xodimi tomonidan siyosatning 9-ilovasida keltirilgan ma’lumotlarni saqlash vositalari, mobil qurilmalar, ma'lumotlar disklari bilan ishlashda xavfsizlikni ta'minlash bo'yicha yo'riqnomaga muvofiq amalga oshiriladi.

39. Zaxira nusxalari va elektron arxivlarning tashqi tashuvchilari siyosatning 13-ilovasida keltirilgan Axborot aktivlarini boshqarish tartibi talablariga muvofiq axborot aktivlari sifatida belgilanadi. Tashqi zaxiraviy tashuvchilar va elektron arxivlarni belgilash uchun javobgarlik ularning saqlanishiga mas'ul bo'lgan Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimi zimmasiga yuklanadi.

40. Zaxira nusxalar yong'in o'chirish tizimlari bilan jihozlangan va ruxsatsiz kirishning oldini olish uchun asosiy va zaxira ma'lumotlarni qayta ishlash markazlarining asosiy server xonalaridan imkon qadar alohida xonalarda saqlanishi kerak.

41. Zaxira va elektron arxivlar uchun tashqi vositalar ikki nusxada bo'lishi kerak. Bitta nusxasi Xavfsizlik va axborotlarni muhofaza qilish departamenti xonalarida joylashgan yopiq yong'inga qarshi seyfda, ikkinchi nusxasi normativ hujjatlar talablariga muvofiq elektron arxivlarni yuritish uchun hujjatlar joylashuv jihatdan uzoq joyda tashkil etilgan xonaning alohida xonasida yopiq yong'inga qarshi seyfda saqlanishi kerak.

42. Zaxira tashuvchilarni hisobdan chiqarish va yo‘q qilish siyosatning 9-ilovasida keltirilgan ma’lumotlarni saqlash tashuvchilar, mobil qurilmalar, ma’lumotlar disklari bilan ishlashda xavfsizlikni ta’minlash bo‘yicha yo‘riqnomaga muvofiq amalga oshiriladi.

IX. Zaxira natijalarini nazorat qilish

43. Barcha zaxiraviy jarayonlar natijalarini nazorat qilish ushbu nizomning jadvalida ko'rsatilgan zaxiralash uchun mas'ul shaxslar tomonidan amalga oshiriladi.

44. Zaxiralash tartib-qoidalarining natijalarini kuzatish nusxasini yaratgandan so'ng darhol amalga oshiriladi.

45. Bank axborot tizimlarining ma’lumotlar bazalarini zaxiralash tartib-taomillari natijalarini nazorat qilish jadvalda ko‘rsatilgan zaxira va tiklash tizimlari tomonidan amalga oshiriladi.

46. Zaxiralash natijalarini kuzatishda quyidagilar tekshiriladi:

barcha nusxa ko'chirish protseduralarini to'g'ri bajarish, ya'ni. nusxa

ko'chirishda xatolik yo'q;

ko'chirilgan ma'lumotlar, fayllar, kataloglar ro'yxati;

ko'chiriladigan fayllar hajmining ko'chiriladigan (arxivlanadigan) hajmiga mos kelishi;

antivirus vositalar yordamida zararli dasturlarning yo'qligini tekshirish.

Zaxiralash natijalarini monitoring qilishning belgilangan tartiblari mas'ul shaxs va/yoki mas'ul shaxs nazorati ostidagi ma'lumotlarni zaxiralash va tiklash tizimi tomonidan amalga oshiriladi.

47. Agar xato aniqlansa, zaxira natijalarini monitoring qilish uchun mas'ul shaxs Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar beradi.

48. Agar zaxiradagi xatolar aniqlansa, takroriy nusxa ko'chirish jarayoni ma'lumotlarni qayta ishlashning texnologik jarayonlarini buzmasdan imkon qadar tezroq qo'lda amalga oshiriladi. Agar xatolar yana takrorlansa, sabablar aniqlanadi: zaxira tizimining noto'g'ri ishlashi yoki noto'g'ri konfiguratsiyasi, zaxira vositalarining to'lib ketishi yoki noto'g'ri ishlashi va boshqalar va ularni bartaraf etish choralari ko'riladi.

X. Axborotni tiklash tartibi

49. Zaxira nusxalaridan ma’lumotlarni qayta tiklash axborot tizimi yoki uning tarkibiy qismi ish qobiliyatini yo‘qotgan taqdirda amalga oshiriladi va Axborot texnologiyalari departamenti direktori hamda Xavfsizlik va axborotlarni muhofaza qilish departamenti direktorining ruxsati asosida amalga oshiriladi.

50. Zaxira nusxasini tiklash jarayonida zaxira tizimi bilan birga kelgan hujjatlarda va axborot tizimining dasturiy ta'minot ishlab chiqaruvchisi hujjatlarida tasvirlangan zaxira nusxalaridan ma'lumotlarni tiklash bo'yicha ko'rsatmalarga amal qilinadi.

51. Axborot tizimlarining ishlashini tiklash rejalarida ko'rsatilgan ma'lumotlarni qayta tiklash imkon qadar tezroq amalga oshiriladi.

52. Zaxira ma'lumotlarining tiklanishini tekshirish tartibi ular qayta tiklangandan so'ng darhol amalga oshiriladi.

53. Qayta tiklashdan keyin zaxiralangan ma'lumotlarni tekshirishda quyidagilar amalga oshiriladi:

barcha tiklash tartib-qoidalarining to'g'riligini tekshirish, ya'ni. bajarilgan protseduralar ro'yxati va ularni amalga oshirishda xatolar yo'qligi;

ko'chirilgan ma'lumotlar, fayllar, kataloglar ro'yxati;

tiklangan fayllar hajmiga muvofiqligi, ya'ni. ma'lumotlarning yaxlitligi tegishli ilovalarda fayllarni birma-bir ochish orqali baholanadi;

virusga qarshi vositalar yordamida tiklangan ma'lumotlarda zararli dasturlarning yo'qligini tekshirish.

Zaxiralangan ma'lumotlarni qayta tiklashning to'g'riligini tekshirish bo'yicha ko'rsatilgan protseduralar mas'ul shaxs va / yoki ma'lumotlarni zaxiralash va tiklash tizimi mas'ul shaxs nazorati ostida amalga oshiriladi.

54. Agar xato aniqlansa, zaxiraviy ma'lumotlarning tiklanishini tekshirish uchun mas'ul shaxs Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar beradi.

55. Zaxiralangan ma'lumotlarni qayta tiklashda xatolar aniqlansa, ikkinchi tiklash jarayoni amalga oshiriladi. Agar xatolar yana takrorlansa, sabablar aniqlanadi: zaxira tizimining noto'g'ri ishlashi yoki noto'g'ri konfiguratsiyasi, zaxira vositalarining to'lib ketishi yoki noto'g'ri ishlashi va boshqalar va ularni bartaraf etish choralari ko'riladi.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
7-ilova

Parol bilan himoya qilish va autentifikatsiya bo‘yicha yo’riqnoma

I. Umumiy qoidalar

1. Ushbu yo‘riqnoma “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda - Bank) xavfsizlik obyektlariga kirishda parolni himoya qilish va autentifikatsiya qilish tartibini, shakllantirish va ulardan foydalanish qoidalarini, shuningdek, talablarni belgilaydi.

2. Ushbu yo‘riqnoma himoyalangan obyektlarga kirish uchun parolni himoyalash va boshqa identifikatorlarni yaratuvchi va boshqaruvchi xodimlarga, shuningdek, bankning ushbu obyektlarga kiruvchi barcha xodimlariga nisbatan qo‘llaniladi.

3. Bank xodimlarining axborot resurslari va tizimlaridan foydalanishi matritsani ishlab chiqish qoidalariga muvofiq ishlab chiqilgan Axborot resurslaridan foydalanish matritsasiga (keyingi o‘rinlarda Matritsa deb yuritiladi) qoidalarga muvofiq chegaralanishi kerak. siyosatga 10-ilovada keltirilgan axborot resurslaridan foydalanish matritsasini ishlab chiqish qoidalari.

II. Atamalar, ta’riflar va qisqartmalar

4. Ushbu yo‘riqnomada quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

1) **avtorizatsiya:** ma'lum bir shaxsga yoki odamlar guruhiga muayyan harakatlarni amalga oshirish huquqini berish.

2) **autentifikatsiya:** foydalanuvchi, dastur, qurilma yoki ma’lumotlarning shaxsini aniqlash tartibi;.

3) **identifikatsiya:** subyektlar va kirish obyektlariga identifikatorni tayinlash va/yoki taqdim yetilgan identifikatorni tayinlangan identifikatorlar ro‘yxati bilan taqqoslash.

4) **initsializatsiya paroli** - foydalanuvchiga dastlabki kirish uchun berilgan parol;

5) **parolni buzish:** ruxsatsiz shaxslarga parolni bilish yoki uni shakllantirish prinsipi.

6) **parol bilan himoya qilish**: tizimga va uning resurslariga parollar orqali kirish jarayonini boshqarish;

7) **parol**: foydalanuvchini tasdiqlash uchun foydalaniladigan maxfiy belgilar to‘plami;.

8) **qayd yozuvi** - axborot tizimlari va manbalariga kirishda foydalaniladigan foydalanuvchi identifikatori.

III. Umumiy talablar

5. Bank xodimlariga quyidagi himoya obyektlariga kirishni ta'minlashda parolni himoyalash va autentifikatsiyadan foydalanish kerak:

1) MBXO va Bankda jismoniy kirish uchun SKUD biometrik ma'lumotlariga asoslangan bir faktorli yoki ikki faktorli autentifikatsiya parol orqali 3 zona va 2 zonali qo'riqlanadigan binolariga, shu jumladan asosiy va zaxira ma'lumotlarni qayta ishlash markazlarining server xonalariga;

2) quyidagilardan foydalanish yoki mantiqiy kirish uchun login va parolga asoslangan bir faktorli autentifikatsiya:

bank ish stansiyalari va lokal/korporativ tarmog'i va bank xodimlarining ish stansiyalariga;

server uskunalari, tarmoq uskunalari va axborot xavfsizligi vositalari - administratorlar (xizmat ko'rsatuvchi xodimlar) tomonidan;

CRM, ELMA BPM, CROBS, SAP, DWH, EDI, Way4 protsessing tizimi va SWIFT tizimi axborot tizimlari - bank xodimlari;

3) login va parolga asoslangan ikki faktorli autentifikatsiya, shuningdek mantiqiy kirish uchun raqamli imzo:

ABT bank ;

yuridik shaxs bo'lgan bank mijozlari interaktiv bank xizmatlaridan foydalanganda internet-Banking va mobil Banking tizimi;

Bank ERI kalitlarini ro'yxatdan o'tkazish markazi – Markaz administratori tomonidan;

E-xat xavfsiz elektron pochta tizimi - bank xodimlari tomonidan;

4) login va parol asosida ikki faktorli autentifikatsiya, shuningdek, interaktiv bank xizmatlaridan foydalanganda jismoniy shaxslar bank mijozlari tomonidan mobil bank tizimiga mantiqiy kirish uchun SMS-kod.

6. Xodimlar ABTga kirishda ERIni tekshirish, shuningdek, mijozlar Internet-Banking va mobil Banking xizmatlariga kirishda ERIni tekshirish uchun bank ERI kalitlarini ro'yxatga olish markazida berilgan va saqlanadigan ERI ochiq kalit sertifikatlaridan foydalaniladi.

7. ERI yopiq kalitlari va ERI ochiq kalit sertifikatlarini yaratishda bank ERI kalitlarini sertifikatlashtirish markazi O'Z DSt 081: 1092:2009 "Axborot texnologiyalari. Axborotni kriptografik himoyalash. Elektron raqamli imzoni yaratish va tekshirish jarayonlari" va O'ZDSt 081 1108:2011 "Axborot texnologiyalari. Ochiq tizimlarning aloqasi. ERI ochiq kaliti sertifikati va atribut sertifikatining tuzilishi.

8. Parollar, ERI shaxsiy kalitlari va SMS kodlari (keyingi o'rinlarda kirish identifikatorlari deb yuritiladi) konfidensial ma'lumotlar bo'lib, ularni oshkor qilish yoki hech kimga topshirish mumkin emas. Ularning egalari ularni xavfsiz saqlash uchun javobgardir.

9. Bank xodimlarining ish stansiyalari foydalanuvchi 5 daqiqa davomida harakatsiz qolganda ekranni avtomatik ravishda blokirovka qilish va uyqu rejimiga - 20 daqiqaga o'tish uchun sozlanishi kerak. Qulflash va uyqu rejimidan chiqish kirish paroli yordamida amalga oshirilishi kerak.

IV. Parollar va boshqa identifikatorlar uchun xavfsizlik talablari

10. Bank xodimlari bank qo‘riqlash vositalariga kirishda shaxsiy parol sir saqlanishi uchun shaxsan javobgardirlar. Parolni boshqa shaxslarga oshkor qilish, shuningdek, yozib olingan parolni jamoat joylarida saqlash taqiqlanadi.

11. Bank xodimining o‘z parollarini qog‘ozda saqlashiga faqat shaxsiy seyfda yoki bank tarkibiy bo‘linmasi rahbarining seyfida yoki muhrlangan, qulflanadigan shkafda.

12. Bank serverlari, tarmoq uskunalari va axborot xavfsizligi vositalarining o‘rnatilgan administrator qayd yozuvi parollari yong‘inga chidamli seyf yoki shkafda xavfsiz joyda saqlanishi kerak. Ushbu parollarga kirish faqat Axborot texnologiyalari departamenti va Xavfsizlik va axborotlarni muhofaza qilish departamentining tarkibiy bo‘linmalari rahbarlarining roziligi bilan amalga oshiriladi.

13. Zarurat tug‘ilganda (xizmat safari, ta’til va h.k.), administratorlar tomonidan olib boriladigan tekshirish tadbirlarida va bank xodimining parolini bilishni talab qilganda, parolingiz qiymatini bevosita rahbariyatingizga oshkor qilishga ruxsat beriladi. Parolni o'tkazish fakti foydalanuvchi tomonidan xavfsizlik maqsadida parolni keyingi o'zgartirishni nazorat qilishda Xavfsizlik va axborotlarni muhofaza qilish departamenti yetkazilishi kerak. Ishlab chiqarish yoki tekshirish ishlari tugagandan so'ng, bank xodimlari mustaqil ravishda yoki administrator orqali "oshkor qilingan" parollarning qiymatlarini darhol o'zgartiradilar.

14. Favqulodda vaziyatlar, fors-major holatlari, shuningdek, yo‘qligida bank xodimlarining ismlari va parollaridan foydalanishning texnologik zarurati yuzaga kelganda, administrator tomonidan ularning parollarini o‘zgartirishga ruxsat etiladi. Bunday hollarda, parollari o'zgartirilgan bank xodimlari parollari o'zgartirilganligini bilgandan so'ng darhol ular uchun yangi parollarga o’zgartirishlari kerak.

15. Bank xodimi uzoq vaqt ishlamagan taqdirda (xizmat safari, kasallik va h.k.) uning foydalanuvchi qayd yozuvi bloklanadi, zarurat tug'ilganda esa boshqa foydalanuvchilarning ushbu bank xodimining resurslariga kirish huquqlari o'zgartiriladi. Uzoq vaqt davomida bo'lmaganlik fakti Xavfsizlik va axborotlarni muhofaza qilish departamentiga xabar qilinishi kerak.

16. Bank xodimlari bo'lgan parol egalari ushbu Yo'riqnomaning imzoga qo’yish orqali talablari bilan tanishishlari va parollardan foydalanish, shuningdek har qanday parol ma'lumotlarini oshkor qilish uchun javobgarlik to'g'risida ogohlantirilishi kerak.

17. Bank xodimlarining ABTga kirishi login va parol, shuningdek, bank xodimiga tegishli bo‘lgan va himoyalangan USB-tashuvchida saqlanadigan shaxsiy ERI kaliti orqali yaratilgan ERI asosida amalga oshiriladi. ERI shaxsiy kalitlari xavfsiz USB-tashuvchida bank xodimiga beriladi.

18. Bank xodimi tomonidan USB-tashuvchilarni ERI yopiq kaliti bilan xavfsiz saqlash ta’minlanadi.

ERI shaxsiy kalitiga kirish faqat o'ziga ma'lum bo'lgan egasining paroli yordamida amalga oshiriladi. Bank xodimlari ushbu yo‘riqnoma ning 7-bo‘limida ko‘rsatilgan talablarga muvofiq ERI yopiq kalitiga kirish uchun murakkab parollardan foydalanishlari shart..

19. Yuridik shaxs bo'lgan bank mijozlariga Internet-Banking va mobil Banking xizmatidan foydalanish uchun himoyalangan USB tashuvchi va ERI

shaxsiy kalitlari beriladi, ular yordamida ular shaxsiy hisoblariga kirish huquqiga ega bo'ladilar va to'lov harakatlarini tasdiqlaydilar.

Bank mijozlarining xavfsizligini ta'minlashga qo'yiladigan talablar ular tomonidan chiqarilgan himoyalangan USB-tashuvchilar va shaxsiy ERI kalitlari interaktiv bank xizmatlarini ko'rsatish shartnomalarida belgilanadi.

20. Bank xodimlari ochiq ERI kalitlari kalitlari va sertifikatlarini berish to‘g‘risidagi bank xodimining arizasida belgilangan himoyalangan USB-tashuvchi va shaxsiy ERI kalitlari xavfsizligini ta’minlash bo‘yicha talablarga rioya etishlari shart.

V. Parollar, ERI shaxsiy kalitlari va ERI ochiq kalit sertifikatlarini yaratish uchun tashkiliy va texnik foaliyat bilan ta’minlash

21. Bank yangi xodimlarining ish stansiyalariga (bankning lokal va korporativ tarmoq) kirishlari uchun qayd yozuvi (login) va ishga tushirish paroli shakllantiriladi

Foydalanuvchi qayd yozuvini ma'lumotlari (login) va ishga tushirish paroli domen boshqaruvchisi serverida Axborot texnologiyalari departamenti Active Directory tizim administratori tomonidan ishlab chiqariladi va yangi xodimga ishga qabul qilish to'g'risidagi buyruq asosida beriladi.

22. Yangi xodimlarning bank axborot tizimlariga kirishi uchun login va ishga tushirish paroli Axborot texnologiyalari departamenti axborot tizimlari administratorlar tomonidan, ABT uchun esa – Buxgalteriya hisobi va moliyaviy menejment departamenti ABT tizim administratori tomonidan shakllantiriladi.

23. Internet-Banking va mobil Banking xizmatlaridan foydalanish uchun bank mijozlari bank tizimida ro'yxatdan o'tishda login va parolni o'zlari shakllantiradilar.

24. Bank xodimlari uchun ishga tushirilgan parollarni yaratish jarayonlarini texnik qo‘llab-quvvatlash sifatida parol generatorlari Passwordgenerator dasturidan foydalaniladi.

25. Ish stansiyalariga (lokal/korporativ tarmoq) kirish uchun ishga tushirilgan parol bankning yangi xodimiga yoki korporativ IP-telefoniya orqali xabar qilinadi.

Bank xodimiga axborot tizimlariga kirish uchun ishga tushirilgan parol korporativ elektron pochta va korporativ IP-telefoniya orqali taqdim etiladi.

26. Initsializatsiya parolidan foydalangan holda bankning lokal/ korporativ tarmog'iga va / yoki axborot tizimlariga kirgandan so'ng, yangi xodim ushbu Yo'riqnomaning 7-bo'limida belgilangan parollarni yaratish talablari va qoidalariga rioya qilgan holda o'z parolini kiritishi kerak.

27. Ruxsatsiz shaxslarning server, tarmoq uskunalari va axborot xavfsizligi vositalariga kirishini cheklash uchun ularga kirish uchun parollar, shuningdek ularga masofaviy kirishni ta’minlovchi ish stansiyalari ularning ishlashi uchun mas’ul xodimlar – administratorlar tomonidan shakllantiriladi va foydalaniladi. Ushbu parollar administratorlarning o'zlari tomonidan ushbu Yo'riqnomaning 7-bo'limida ko'rsatilgan talablarga muvofiq ishlab chiqariladi.

28. ABT tizimiga kirish uchun ABT foydalanuvchisi bo'lgan bank xodimlari bank rahbariyatiga so'rovlar (arizalar) yuborishlari kerak.

29. Bank rahbariyati ABTga kirish uchun so‘rovlarni (arizalarni) ma’qullagandan so‘ng, Buxgalteriya hisobi va moliyaviy menejment departamentining ABT tizimi administratori qayd yozuvi yaratadi va kirish parolini (boshlang‘ich parol), Xavfsizlik va departamentining axborotni himoya qilish boshqarmasi esa bank xodimlari uchun ERI shaxsiy va ochiq kalitlarini ishlab chiqaradi.

30. Xodimlar ABT ga kirishda ERIni yaratish uchun foydalaniladigan ERI shaxsiy kalitlari va ERI ochiq kalit sertifikatlari Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoya qilish boshqarmasi mas’ul xodimi tomonidan ishlab chiqariladi.

31. ERIning shaxsiy kalitini yaratish va ochiq ERI kalitini shakllantirish bank ERI kalitlarini ro‘yxatga olish markazi dasturiy ta’minoti bilan ta’minlanadi.

32. Yaratilgan ERI shaxsiy kalitlari xavfsiz USB-tashuvchiga yoziladi.

33. Xavfsiz USB-tashuvchidagi ERI shaxsiy kalitlari xodimlarga qabul qilish sertifikatlari bilan beriladi, ularda:

xodimning to'liq ismi va lavozimi;

asosiy axborot tashuvchining seriya raqami;

chiqarilgan sana va vaqt;

himoyalangan USB tashuvchining xavfsizligini ta'minlash bo'yicha xodimning majburiyatlari.

Bank xodimlariga xavfsiz USB-tashuvchini berish jurnaldagi imzo bilan amalga oshiriladi.

34. Xavfsiz USB-tashuvchida ERI shaxsiy kalitlari chiqarilgunga qadar ular Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoya qilish boshqarmasi seyfida saqlanishi kerak.

35. ERI ochiq kalitlari sertifikatlari bank ERI kalitlarini ro‘yxatga olish markazining ma’lumotlar bazasiga kiritilgan.

VI. Parollar va boshqa identifikatorlarni o'zgartirish va tugatish jarayonlari

36. Bank xodimlari ish stansiyalariga (bank lokal/korporativ tarmog‘i) kirishda kamida oyiga bir marta parolini (rejalashtirilgan parolni o'zgartirish) o‘zgartirishlari shart. Ushbu talab foydalanuvchi qayd yozuvini boshqarish uchun bank domen kontrolleri serverining Windows Server Active Directory xizmatining tegishli sozlamalari bilan ta’minlanishi kerak.

37. Bank xodimlari axborot tizimlariga kirishda har oyda kamida bir marta parolni (rejalashtirilgan parolni o'zgartirish) o‘zgartirishlari shart.

Ushbu talab axborot tizimlarida foydalanuvchilarning kirishini boshqarish tizimidagi tegishli sozlamalar bilan ta'minlanishi kerak.

38. Bank axborot tizimlarida domen kontroller serverlari Active Directory xizmati va foydalanuvchilardan foydalanishni boshqarish tizimlari sozlamalarida bank xodimlari tomonidan parolni o‘zgartirish bo‘yicha quyidagi talablar bajarilishi kerak:

foydalanuvchi tomonidan vaqti-vaqti bilan parolni o'zgartirish;

ushbu Yo'riqnomaning 7-bo'limi talablariga muvofiq kiritilgan parolning murakkabligi;

yangi kiritilgan parol xodim tomonidan ilgari kiritilgan beshta parolni takrorlamasligi kerak.

39. Serverga, tarmoq uskunasiga va axborot xavfsizligi vositalariga kirish uchun parollarni rejali ravishda o'zgartirish ularning ishlashi uchun mas'ul bo'lgan administrator tomonidan kamida 3 oyda bir marta amalga oshirilishi kerak.

Administratorlar tomonidan parolni davriy o'zgartirish talabiga rioya etilishi Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan nazorat qilinadi.

40. Foydalanuvchi parolini rejadan tashqari o'zgartirish quyidagi hollarda amalga oshiriladi:

foydalanuvchi parolining buzilganligi yoki shubhali holat;

foydalanuvchining vakolatini tugatish (ishdan bo'shatish, boshqa ishga o'tkazish va boshqalar);

axborot tizimi administrator va o'z faoliyati xususiyatiga ko'ra parol bilan himoya qilishni boshqarish vakolati berilgan boshqa xodimlarning vakolatlarini tugatish (ishdan bo'shatish, boshqa ishga o'tkazish va boshqa holatlar).

41. Parol buzilgan yoki shubhali bo'lgan taqdirda, bank xodimi hisobga kirishni bloklash va yangi ishga tushirish parolini yaratish uchun Axborot texnologiyalari departamentiga yoki Buxgalteriya hisobi va moliyaviy menejment departamentiga (ABT tizimi uchun) xabar berishi kerak.

42. Administrator foydalanuvchi qayd yozuvining paroli buzilgan yoki shubhali buzilgan taqdirda, administrator uni darhol o'zgartirishi shart.

43. ERI yopiq kalitlarini rejalashtirilgan o'zgartirish Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoya qilish boshqarmasi tomonidan ERI ochiq kaliti sertifikatining amal qilish muddatidan kelib chiqqan holda har 2 yilda bir marta amalga oshirilishi kerak.

44. ERI konfidensial kaliti buzilgan yoki shubhali bo'lgan taqdirda, bank xodimi ERI ochiq kaliti sertifikatining amal qilishini to'xtatib turishi yoki bekor qilishi va yangi yopiq kalit sertifikat yaratishi kerak bo'lgan Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoya qilish boshqarmasiga darhol xabar berishi shart.

45. Parol va ERI yopiq kalitini rejadan tashqari o'zgartirish, uning vakolatlari tugatilganda (ishdan bo'shatish, boshqa ishga o'tkazish va h.k.) bank xodimining foydalanuvchi qayd yozuvini raqamini va ochiq kalit sertifikatini o'chirish oxirgi tizimdagi ushbu xodimning muddat tugagandan so'ng darhol amalga oshirilishi kerak.

Barcha foydalanuvchilar uchun parollarni rejadan tashqari to'liq o'zgartirish axborot tizimi parol himoyasini boshqarish vakolati administratorlar va o'z ishining xususiyatiga ko'ra berilgan boshqa xodimlarning vakolatlari tugatilgan taqdirda (ishdan bo'shatish, boshqa ishga o'tkazish va boshqa holatlar) amalga oshirilishi kerak.

46. foydalanuvchi qayd yozuvi orqali himoyalangan obyektlarga kirish noto'g'ri parolni kiritish uchun uchta muvaffaqiyatsiz urinishdan keyin bloklanishi kerak.

47. Agar ERI shaxsiy kalitlari bo'lgan himoyalangan USB-tashuvchilar ishlatilmasa (ish kuni tugashi, ta'tilga chiqish yoki kasallik tufayli ta'tiliga chiqish va h.k.), bank xodimi uni o'zining tarkibiy bo'linmasi rahbariga yoki tashkilot rahbariga topshirishi shart. Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni muhofaza qilish boshqarmasi yoki MBXO xavfsizligi va axborotni himoya qilish bo'limiga. bank xodimlarining foydalanilmagan xavfsiz USB-disklari seyflarda saqlanishi kerak.

VII. Parol yaratish talablari

48. Bankda ma’lumot obyektlariga kirish uchun parollarni yaratishda quyidagi talablar amalga oshirilishi kerak:

parolning minimal uzunligi kamida 8 belgidan iborat bo‘lishi kerak;

parol raqamlar kombinatsiyasidan, lotin alifbosidagi katta va kichik harflar, shuningdek belgilardan iborat bo‘lishi kerak.

parolda osongina hisoblangan belgilar kombinatsiyasi (ism, familiya va boshqalar), shuningdek, umumiy qabul qilingan qisqartmalar (LAN, USER va boshqalar) bo‘lmasligi kerak;

parolni o‘zgartirganda uning yangi qiymati avvalgisidan kamida 6 holatda farq qilishi kerak

49. Bank xodimi tomonidan ABT Colvir’da ishlash uchun foydalaniladigan ERI yopiq kalitiga kirish uchun parollarga 38-bandda ko‘rsatilgan talablar qo‘llaniladi.

50. Axborot tizimlari ma’lumotlar bazasi administrator paroli kichik va katta harflar, raqamlar va maxsus belgilar yordamida kamida 12 ta belgidan iborat bo‘lishi kerak.

VIII. Parollar va kriptografik kalitlar bilan ishlashda foydalanuvchilar va xizmat ko‘rsatuvchi xodimlarning xatti-harakatlarini boshqarish

51. Parollar va kriptografik kalitlar bilan ishlashda foydalanuvchilar va texnik xizmat ko'rsatuvchi xodimlarning harakatlarini nazorat qilish Xavfsizlik xizmatining axborot xavfsizligi bo’limi zimmasiga yuklatilgan.

52. Parollar bilan ishlashda foydalanuvchilar va texnik xizmat ko'rsatuvchi xodimlarning harakatlari ustidan nazorat Xavfsizlik xizmatining Axborot xavfsizligi bo’limi tomonidan kamida 6 oyda bir marta amalga oshiriladi.

53. Parollar va kriptografik kalitlar bilan ishlashda foydalanuvchilar va texnik xizmat ko'rsatuvchi xodimlarning harakatlarini kuzatib borishda ular quyidagilarni tekshiradilar:

ushbu yo'riqnomaning 7-bo'limiga muvofiq parollarni yaratishga qo'yiladigan talablar;

ushbu yo'riqnomaga muvofiq parollar va kriptografik kalitlarni saqlashga qo'yiladigan talablar;

parol egalarining ushbu yo'riqnomaning 9-bo'limida belgilangan majburiyatlari;

kriptografik kalitlar egalarining axborotni kriptografik himoyalashni tashkil etish bo‘yicha yo‘riqnomada belgilangan majburiyatlari.

54. Nazorat davomida bank domen kontrolleri serverining Active Directory xizmati va bank axborot tizimlarida foydalanuvchilarning kirishini boshqarish tizimlari sozlamalari to‘g‘riligi tekshiriladi.

Bank xodimlarining parollari xavfsizligini ta'minlash uchun tanlab tekshirish (so'rov, tekshirish).

Administratorlarni ular kiritgan parollarning murakkabligi, ular qanday saqlanishi va parollarni qanchalik tez-tez o'zgartirishi haqida tekshirish.

55. Ushbu Yo'riqnoma talablari buzilgan taqdirda, Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimlari xodimga takroriy buzilishning oldini olish uchun ogohlantirish berishlari shart.

56. Mazkur yo‘riqnoma talablarining muntazam yoki qo‘pol ravishda buzilganligi holatlari to‘g‘risida bank rahbariyatiga qoidabuzarga nisbatan tegishli choralar ko‘rishlari uchun xabar qilinadi.

IX. Majburiyatlari

57. Parol egalarining majburiyatlari:

turli xil axborotlashtirish obyektlariga kirishda har xil parollarni qo‘llash;

qayd yozuvidagi eski parolni blokirovka qilish, parolni rejadan tashqari o‘zgartirishni blokirovka qilish, axborot xavfsizligi administratoriga uning paroli buzilganligi to‘g‘risida xabar berish;

parol xavfsizligini ta’minlash;

qayd yozuvi parollarini boshqa xodimlarga va ruxsatsiz shaxslarga bermaslik.

58. Parol egasi o‘z parollarini himoya qilish uchun tegishli choralarni ko‘rishi kerak, shu jumladan:

parollarni eslab qolish yoki ularni boshqa shaxslar yashirish;

parollarni hech kimga, shu jumladan hamkasblarga, tarkibiy bo‘linmaning bevosita rahbariga bermaslik;

paroldan foydalanganda (masalan, uni kiritishda), uning parol kompрometatsiyasini oldini olish uchun zarur choralarni ko‘rish (masalan, kiritilgan parolni vizual ko‘rish imkoniyatini cheklash).

59. Bank tizimlarida ishlatiladigan parollarni tashqarida (masalan, internet saytlarida, internet-do‘konlarda, elektron to‘lov tizimlarida va boshqalar) foydalanish ta’qiqlanadi.

60. ERI yopiq kalitlari egalarining majburiyatlari siyosatning 15-ilovasida keltirilgan kriptografik axborotni muhofaza qilishni tashkil etish bo‘yicha yo‘riqnomada belgilangan va bank xodimlari tomonidan bajarilishi shart.

61. Yuridik shaxslar Banklari mijozlarining o'z parollari, himoyalangan USB-tashuvchilari ERI yopiq kalitlari bilan birgalikda interaktiv Bank xizmatlarini ko'rsatish bo'yicha ular bilan tuzilgan shartnomalarda saqlanishi bo'yicha majburiyatlari va javobgarliklari belgilanishi kerak.

62. Administratorlarga foydalanuvchi parollarini aniq matnda saqlash, shuningdek, umumiy foydalanish manbalarida parollarni joylashtirish yoki ularni elektron pochta orqali yuborish taqiqlanadi, foydalanuvchiga ishga tushirish parolini

yuborish bundan mustasno (faqat korporativ elektron pochta yoki korporativ telefon orqali).

63. Xavfsizlik va axborotlarni muhofaza qilish departamenti quyidagilarga majburdir:

xodimlarga parolni himoyalash va boshqa identifikatorlardan foydalanish, ularning xavfsizligini ta'minlash va ularning murosaga kelishi uchun javobgarlik bo'yicha maslahat berish;

bank xodimlari tomonidan mazkur yo‘riqnomani buzganlik holatlari to‘g‘risida zudlik bilan Xavfsizlik va axborotlarni muhofaza qilish departamenti direktorini xabardor qilish.

X. Javobgarlik

64. Parollarni yaratuvchi xodimlar va administratorlar ushbu Yo'riqnoma talablariga rioya qilish uchun javobgardirlar.

65. Bank xodimlari ushbu yo‘riqnoma talablariga muvofiq o‘z parollari va qo‘riqlanadigan obyektlarga kirishning boshqa identifikatorlarining saqlanishini ta’minlash uchun javobgardirlar.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
8-ilova

Antivirus himoyasi bo‘yicha yo’riqnoma

I. Umumiy qoidalar

1. “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank)ning Antivirus himoyasi bo‘yicha ushbu yo’riqnomasi quyidagilarni belgilaydi:

bankning axborot va bank axborot-kommunikatsiya infratuzilmasini zararli dasturlar harakatlaridan himoya qilishni tashkil etish tartibi;

bank xodimlari tomonidan bajarilishi shart bo‘lgan zararli dasturlardan himoyalanish talablari;

antivirus himoya qilish tartib-qoidalarini amalga oshirishda bank xodimlarining burch va majburiyatlari.

2. Ushbu yo‘riqnoma bankning barcha xodimlari, bankning bank axborot infratuzilmasidan foydalanishda, shuningdek, Bankda virusga qarshi himoyani ta’minlashga mas’ul bo‘lgan xodimlar uchun majburiy hisoblanadi.

II. Atamalar, ta’riflar va qisqartmalar

3. Ushbu yo‘riqnomada quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

1) **antivirus himoyasi:** antivirus dasturlari yordamida kompyuter virusining oldini olish, aniqlash va zararsizlantirishga qaratilgan chora-tadbirlar majmui;

2) **antivirus dasturi:** viruslar, o’rgimchak tarmoq, troyanlar, fishing havolalari va boshqalarni o'z ichiga olgan zararli dasturlarni aniqlash, davolash va yo'q qilish mexanizmini o'z ichiga olgan maxsus dasturiy ta'minot;

3) **antivirus nazorati:** ish stansiyalari va serverlarida zararli dasturlarni muntazam tekshirish, kunlik yangilanishlar, har oyda ish stansiyalari va serverlarni zararli dasturlarga to'liq tekshirish, zararli dasturlarni aniqlash bilan bog'liq hodisalarga javob berish;

4) **antivirusni boshqarish vositasi -** parametrlarni markazlashtirilgan nazorat qilish, virusga qarshi vositani yangilash va virusga qarshi himoya sohasidagi hodisalarni boshqarish uchun avtomatlashtirilgan tizim;

5) **zararli dastur:** apparat, dasturiy-apparat yoki dasturiy ta'minotda amalga oshirilgan va har qanday ruxsatsiz yoki zararli faoliyatni amalga oshirish uchun mo'ljallangan dastur.

III. Umumiy talablar

4. Bankda antivirus vositasi va axborotni qayta ishlash vositalarini zararli dasturlardan himoya qilish maqsadida antivirus himoyasi tashkil etilgan.

5. Bank virusdan himoya qilish bo‘yicha quyidagi chora-tadbirlar va vositalarni qo‘llaydi:

a) ma'lumotlarni qayta ishlash vositalarida ularni aniqlash va blokirovka qilishni, asl holatini tiklashni ta'minlaydigan, shuningdek foydalanuvchilarni xabardor qilish uchun mo'ljallangan zararli dasturlardan (antiviruslardan) foydalanish;

b) bankda ushbu yo‘riqnoma da belgilangan va bank xodimlari tomonidan bajarilishi shart bo‘lgan virusga qarshi himoya talablarini belgilash;

c) zararli dasturlardan tarmoq trafigini himoya qilish vositalaridan (IDPS hujumlarini aniqlash va oldini olish vositalari) foydalanish;

d) zararli dasturlardan foydalanish mumkin bo'lgan zaifliklarni aniqlash va yo'q qilish;

e) zararli web-resurslarga kirishni bloklash, bunday web-resurslar ro'yxatini tuzish va yuritish;

f) antivirus yordamida ma'lumotlarni qayta ishlash vositalarida USB portlaridan foydalanishni blokirovka qilish, ulardan rasmiy vazifalarni bajarish uchun ulardan foydalanish talab etilmaydi (ariza asosida USB portlariga kirish bank rahbariyatining ruxsati bilan xodimlarga beriladi.);

g) ruxsat etilmagan dasturlarni ishchilar tomonidan o'z ish stansiyalarida o'z-o'zidan o'rnatish imkoniyatini cheklash;

h) xavfsizlikni yaxshilash uchun tegishli web-brauzer sozlamalarini o'rnatish;

i) Bank xodimlarining virusga qarshi himoya masalalari bo'yicha xabardorligini oshirish bo'yicha treninglar o'tkazish.

6. Axborot xavfsizligini ta’minlash maqsadida Bankda faqat litsenziyalangan antivirusga qarshi vositalardan foydalanishga ruxsat berilgan.

7. Bankning bank axborot-kommunikatsiya infratuzilmasiga antivirusga qarshi vositalar o‘rnatilmagan ish stansiyalari va serverlarini ulashga yo‘l qo‘yilmaydi.

8. Bank antivirusga qarshi dasturlarni markazlashgan holda boshqarishning litsenziyalangan tizimidan (keyingi o‘rinlarda markazlashtirilgan antivirus tizim deb yuritiladi) foydalanadi.

Ushbu antivirus tizimi quyidagilardan iborat:

asosiy ma'lumotlarni qayta ishlash markazida o'rnatilgan markaziy server, undan bankda antiviruslarni markazlashtirilgan yangilash amalga oshiriladi va ulardan antivirus xavfsizligini buzish holatlari to'g'risida ma'lumotlar yig'iladi;

MBXOdagi ish stansiyalarida o'rnatilgan antiviruslarning ishlashi va boshqaruvini nazorat qilish uchun har bir MBXOda yordamchi serverlar va unga bo'ysunuvchi BXM, masofaviy kassalar, ushbu server MBXO server xonasida joylashgan;

har bir ish stansiyasida o'rnatilgan antiviruslar va Bankda foydalaniladigan serverlar

9. Shuningdek, bankning ish stansiyalarida o'rnatilgan antiviruslarda tarmoqlararo ekran (Anti-hacker) funksiyasi qo'shimcha ravishda sozlangan.

10. Barcha ish stansiyalari, serverlar va tarmoq trafigi majburiy antivirus nazorati ostida.

11. Bundan tashqari, bank tarmoq trafigida zararli dasturlarni aniqlash va zararsizlantirish funksiyasiga ega IDPS vositalaridan foydalanadi. Ushbu vositalar

bank korporativ tarmog‘ini tashqi tarmoqlarga ulash chegarasida o‘rnatilgan bo‘lib, kiruvchi tashqi trafikda zararli dasturlar mavjudligi tekshiriladi.

12. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi Bankda antivirusning kelib chiqishi va uning turini ko‘rsatgan holda kompyuter antivirusi aniqlanganligi to‘g‘risida O‘zbekiston Respublikasi Markaziy bankiga ma’lum qiladi.

IV. Antivirus himoyasi ishlarini tashkil etish

13. Bankda antivirus himoyasi bo‘yicha ishlarni tashkil etish uchun Xavfsizlik va axborotlarni muhofaza qilish departamenti mas’ul hisoblanadi.

14. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasining antivirus himoyasi ta'minlash bo'yicha vazifalariga quyidagilar kiradi:

antivirus himoyasini tashkil etish - antivirus himoyasi choralari va vositalarini amalga oshirish;

antivirus sozlamalari to'g'riligini, shuningdek, xodimlarning ish stansiyalarida yoki muhim biznes jarayonlarini qo'llab-quvvatlaydigan ma'lumotlarni qayta ishlash vositalarida dasturiy ta'minot inventarlarini muntazam ravishda tekshirish;

zararli dasturlar tomonidan qo'llaniladigan zaifliklarni qidirish va yo'q qilish;

bank xodimlari tomonidan virusdan himoyalanish talablariga rioya etilishini nazorat qilish.

15. Bankda markazlashtirilgan antivirus himoyasi tizim administratori Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan, MBXOda esa – MBXOning Xavfsizlik va axborotni muhofaza qilish bo‘limlari tomonidan amalga oshiriladi.

Ish stansiyalari va serverlarida antiviruslarni o'rnatish va sozlash Axborot texnologiyalari departamentining Texnik ta'minot va texnik jihozlarni hisobga olish bo'limi xodimlari tomonidan, MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda esa - MBXO Axborot texnologiyalari bo'limi xodimlar tomonidan amalga oshiriladi.

16. Antivirus himoyasini sozlashda quyidagi talablarga rioya qilish kerak:

antivirus himoyasini ma'lumotlar bazasining doimiy yangilanishini ta'minlash va antivirus himoyasi vositalarining ishlashini nazorat qilish;

bank xodimlari va administratorlar tomonidan antivirusni o'chirish, antivirus himoyasi vositalar sozlamalarini o'zgartirish yoki ularni olib tashlashni taqiqlash;

axborotni qayta ishlash vositalarini davriy ravishda to'liq skanerlash;

zararli dastur ta'sirini mahalliylashtirish va yo'q qilish, zararli dastur bilan zararlangan vositalarni izolyatsiya qilish;

markazlashtirilgan antivirus himoyasi tizim administratorini xabardor qilish uchun jurnallar va ogohlantirishlarni taqdim etish;

antivirus yordamida ma'lumotlarni qayta ishlash vositalarida USB portlaridan foydalanishni bloklash, ulardan foydalanish talab qilinmaydi.

Ushbu talablarga rioya etilishi Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan nazorat qilinadi.

17. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan boshqariladigan IDPS vositalarining sozlamalari zararli dasturlar uchun trafikni kuzatish uchun sozlanishi kerak.

18. Disklarning barcha yuklash sektorlari va axborotni qayta ishlash vositalarining fayllarini antivirus nazorati har kuni avtomatik rejimda ish stansiyalarini dastlabki yuklash paytida yoki ma'lum bir vaqtda (tushlik tanaffus) va serverlar - ular qayta ishga tushirilganda amalga oshirilishi kerak.

19. Ish stansiyalari va serverlarida o'rnatilgan antivirus vositalarining ma'lumotlar bazalarini yangilash markazlashtirilgan antivirus tizimidan avtomatik rejimda muntazam ravishda amalga oshirilishi kerak. Markazlashtirilgan antivirus tizimi antivirus sotuvchisining yangilanish serverlariga kirish uchun sozlanishi kerak.

20. Majburiy antivirus nazorati bankning korporativ va lokal tarmoqlari, shuningdek, saqlanadigan tashuvchilar orqali olingan va uzatiladigan har qanday ma'lumotlar (har qanday formatdagi matnli fayllar, ma'lumotlar fayllari, bajariladigan fayllar) bo'ysunadi.

21. Elektron arxivga joylashtirilgan fayllar antivirus himoyasidan nazoratdan mutlaqo o'tishi kerak. Elektron arxivlarni davriy tekshirish kamida oyiga bir marta amalga oshirilishi kerak.

22. Axborotni qayta ishlash vositalariga tizimli va amaliy dasturiy ta'minotni o'rnatish (o'zgartirish) Axborot texnologiyalari departamentining texnik ta'minlash va texnik jihozlarni hisobga olish bo'limi xodimlari tomonidan amalga oshiriladi. O'rnatilgan (o'zgartirilgan) dasturiy ta'minot zararli dasturlarning yo'qligi uchun oldindan tekshirilishi kerak. Tizim dasturiy ta'minotini o'rnatgandan (o'zgartirgandan) so'ng darhol antivirus himoya vositasidan tekshiruvdan o'tkazilishi kerak.

23. Bank xodimlariga o'z ish stansiyalariga dasturiy ta'minotni mustaqil ravishda o'rnatishga yo'l qo'ymaslik uchun ularga o'z ish stansiyalariga foydalanuvchi (administrator emas) kirishi ta'minlanishi kerak.

V. Antivirusdan himoya qilish ishlarining ishtirokchilariga qo'yiladigan talablar

24. Ishchi stansiyalari va serverlarini o'rnatilgan antivirus dasturisiz ishlatish ta'qiqlanadi. Antivirus dasturini yangilab turish kerak.

Antivirus himoya dasturini yangilanib turishi nazorat qilinadi.

25. Zararli dasturiy ta'minot mavjudligiga shubha bo'lsa (dasturlarning g'ayrioddiy ishlashi, grafik va ovoz effektlarining paydo bo'lishi, ma'lumotlarning buzilishi, fayllarning yo'qolishi, tizim xatosi haqida xabarlarning tez-tez paydo bo'lishi), bank xodimi yolg'iz yoki xodim bilan birgalikda. Axborot texnologiyalari departamentining Texnik ta'minot va buxgalteriya bo'limi yoki MBXOning Axborot

texnologiyalari bo'limi o'z ish stansiyasini virusga qarshi nazoratni amalga oshirishi kerak.

26. Agar antivirus tekshiruvi paytida kompyuter viruslari bilan zararlangan fayllar aniqlansa, bank xodimlari quyidagilarga majburdirlar:

ishni to'xtatib turish;

axborot texnologiyalari departamentining Texnik ta'minot va texnik jihozlarni hisobga olish bo'limi yoki MBXOning Axborot texnologiyalari bo'limi xodimlarini, shuningdek, ushbu fayllardan o'z ishlarida foydalanadigan bank xodimlarini darhol xabardor qilish. virus bilan zararlangan fayllarni aniqlash;

undan keyingi foydalanishni tahlil qilish;

zararlangan fayllarni zararsizlantirish yoki yo'q qilish;

qo‘llanilayotgan virusga qarshi vositalar yordamida davolab bo‘lmaydigan yangi virus aniqlangan taqdirda, bu haqda Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasiga xabar berish.

27. Agar ish stansiyasi yoki server kompyuter virusi bilan zararlangan bo‘lsa, uning bank tarmog‘i orqali tarqalishining oldini olish uchun quyidagi operativ chora-tadbirlar ko‘rilishi kerak:

zararlangan ish stansiyasi yoki serverdagi ishni to'xtatib turish va tarmoq kabelini ajratib, uni tarmoqdan uzish;

litsenziyalangan virusga qarshi vosita yordamida virusni qidirish va olib tashlash;

agar virusni antivirus vositasi bilan olib tashlab bo'lmasa, operatsion tizim va ish stansiyasi yoki serverdagi dasturlarni qayta o'rnatish kerak.

28. Ish stansiyasidan foydalanuvchiga quyidagilar taqiqlanadi:

virusga qarshi himoya vositalarining sozlamalari va konfiguratsiyasini o'zgartirish;

tizimga boshqa antivirus himoya vositalarini olib tashlash yoki qo'shish;

o'rnatilgan virusga qarshi himoya vositalarini oldindan tekshirmasdan ish stansiyasida olinadigan saqlash vositalaridan foydalaning;

elektron pochta orqali yuborilgan yoki Internetdan yuklab olingan noma'lum ilovalarni ishga tushirish.

29. Bank xodimi quyidagilarga majburdir:

noma'lum, shubhali yoki ishonchsiz manbalardan olingan elektron pochta xabarlariga qo'shimchalarni ochmaslik. Bunday qo'shimchalar darhol olib tashlanishi kerak;

noma'lum yoki shubhali manbalardan ma'lumotlarni yuklab olmaslik;

o'qish/yozish huquqiga ega bo'lgan ish stansiyasining mantiqiy disklari va fayl papkalarini almashishdan saqlanish, agar bu asosiy faoliyatning bir qismi sifatida talab qilinmasa;

noma'lum yoki shubhali manbalardan olingan saqlash vositasidan foydalanishdan oldin uni viruslar yo'qligi uchun skanerlash;

har kuni ish stansiyasini dastlabki yuklashda rezident antivirus monitori mavjudligiga ishonch hosil qilish va agar u mavjud bo'lmasa, bu haqda Axborot texnologiyalari departamentining Texnik ta'minot va texnik jihozlarni hisobga olish bo'limi xodimiga yoki MBXOning Axborot texnologiyalari bo'limi xodimlariga xabar berish;

Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasidan tizimda virus mavjudligi to'g'risida bildirishnoma olgandan so'ng, shuningdek virusga shubha tug'ilganda ish stansiyasini rejadan tashqari virusga qarshi skanerlashni mustaqil ravishda amalga oshirish;

VI. Antivirus himoya vositasida ishtirokchilarning javobgarligi

30. Ushbu yo'riqnoma talablariga muvofiq antivirus himoya vositasi nazoratni tashkil etish uchun javobgarlik Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi zimmasiga yuklanadi.

31. Ushbu yo'riqnoma talablariga rioya qilish uchun javobgarlik bank xodimlari, Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi boshlig'i va MBXOning Xavfsizlik va axborotni muhofaza qilish bo'limlari rahbarlari zimmasiga yuklanadi.

32. Bank xodimlari tomonidan antivirus himoya vositasi holatining, shuningdek antivirus himoya vositasi nazoratning belgilangan tartibiga rioya etilishi va ushbu yo‘riqnoma talablariga rioya etilishining davriy monitoringi bankni Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan amalga oshiriladi.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
9-ilova

Mobil, ma’lumot saqlovchi va tashuvchi qurilmalar bilan ishlashda axborot xavfsizligini ta’minlash bo’yicha yo’riqnoma

I. Umumiy qoidalar

1. Ushbu yo‘riqnoma “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda - bank)ning axborot xavfsizligini ta’minlash maqsadida mobil qurilmalar, olinadigan tashuvchilar va ma’lumotlar tashuvchilardan foydalanishga qo‘yiladigan talab va qoidalarni belgilaydi.

2. Bankning axborot infratuzilmasida mobil qurilmalar va saqlash vositalaridan foydalanish va mobil qurilmalar, shuningdek, axborot tashuvchilar deganda ularni bank axborot infratuzilmasi o‘rtasida ma’lumotlarni qayta ishlash, qabul qilish/uzatish maqsadida ish stansiyasiga, serverga, lokal va korporativ tarmoqqa, axborot tizimlariga ulash tushuniladi.

II. Atamalar va ta’riflar

3. Ushbu yo‘riqnomada quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

1) **mobil qurilmalar** - smartfonlar, internet-planshetlar, elektron kitoblar, telefonlar, shaxsiy raqamli yordamchilar, operatsion tizimga ega netbuklar va mobil tarmoqlarga, Wi-Fi va internetga ulanish imkonini beradigan mobil ilovalar, shuningdek ish stansiyalari va boshqa shunga o‘xshash qurilmalar;

2) **ma’lumotlarni saqlash qurilmasi** - ma’lumotni zaxiralash va saqlash, shuningdek uni tashish uchun foydalaniladigan ma’lumotni o‘qiydigan yoki yozadigan qurilma;

3) **saqlash vositasi** - oflayn rejimida saqlash uchun mo‘ljallangan va saqlash joyidan mustaqil ravishda foydalanish mumkin bo’lgan qurilmalar. Ular quyidagi shaklda bo‘lishi mumkin: olinadigan qattiq disklar, flesh-xotira, optik lazer disklari (CD, DVD), disketalar.

III. Mobil qurilmalardan foydalanish qoidalari va talablari

4. Bankda mobil qurilmalardan foydalanish qo‘yiladigan ushbu talablar mobil qurilmalar axborot xavfsizligi tahdidlariga, xususan, mobil telefonlar ko‘proq tahdid ekanligini, (videoyozuv, suratga olish, audioyozuv) ma’lumotlarni (yozib olish ma'lumotlarni saqlash va boshqalar) hamda tashqariga chiqarishda samarali foydalanish mumkinligini anglagan holda tuzilgan,

5. Ushbu hujjatda belgilangan talablar quyidagi mobil qurilmalardan foydalanishga nisbatan qo'llaniladi:

a) Bank xodimlari bo‘lmagan shaxslar (mijozlar va tashrif buyuruvchilar) bankka tashrif buyurganlarida;

b) bank xodimlari;

s) bank va bank xodimlariga xizmat vazifalarini bajarishlari uchun;

6. Uchinchi shaxslarga va bank xodimlariga tegishli barcha turdagi mobil qurilmalardan foydalanish taqiqlanadi:

konfidensial muzokaralar va konfidensial tadbirlar o'tkaziladigan xonalarda;

bankning lokal va korporativ tarmoqlariga, shuningdek, axborot tizimlariga ulanishda;

bankning mobil qurilmalarni axborot tizimi va korporativ tarmog‘iga umumiy foydalanishdagi telekommunikatsiya tarmog‘i va internet tarmog‘i orqali masofadan ulash uchun;

konfidensial yoki boshqa himoyalangan ma'lumotlar, shu jumladan elektron raqamli imzoning parollari va kriptografik kalitlari (keyingi o'rinlarda - ERI) tashuvchilari sifatida.

7. Internet tarmog‘iga kirish uchun AB, MBXO va BXM oldi zonalaridagi korporativ va lokal tarmoqlardan jismoniy jihatdan alohida tashkil etilgan Wi-Fi tarmog‘iga ulanish uchun bank mijozlariga tegishli barcha turdagi mobil qurilmalardan foydalanish mumkin.

8. Bankning bank axborot infratuzilmasida faqat bank mulki bo‘lgan va bank xodimlari foydalanishi uchun berilgan ro‘yxatdan o‘tgan mobil qurilmalar – noutbuklardan (keyingi o‘rinlarda – qayd etilgan noutbuklari) foydalanishga ruxsat etiladi. Boshqa turdagi mobil qurilmalar bank xodimlariga ruxsat etilmaydi.

9. Qayd etilgan noutbuklaridan foydalanilganda, ular statsionar ish stansiyalari kabi ma'lumotlarni himoya qilish talablariga bo'ysunadi va virusga qarshi vositalar bilan jihozlangan bo'lishi va zararli dasturlar uchun vaqti-vaqti bilan tekshirilishi kerak.

10. Qayd etilgan noutbuklarni quyidagilar uchun ishlatish taqiqlanadi:

bankning har qanday konfidensial ma’lumotlarini saqlash;

ABTga ulanishlar, shu jumladan nazorat qilinadigan hududda;

umumiy foydalanishdagi telekommunikatsiya tarmog‘i va internet tarmog‘i orqali axborot tizimlariga, shu jumladan ABT, bank korporativ va lokal tarmog‘iga masofadan ulanish.

11. Qayd etilgan mobil noutbuklardan bank axborot tizimlariga ulanish uchun ABTdan tashqari, faqat nazorat qilinadigan hududda foydalanish mumkin. Shu bilan birga, ularga qo'yiladigan talablar ish stansiyalari bilan bir xil.

12. Bank xodimlari qayd etilgan noutbuklaridan foydalanishda quyidagi talablarga rioya qilishlari shart:

ulardan maqsadli va faqat xizmat vazifalarini bajarish uchun foydalanish;

Axborot texnologiyalari departamentiga ushbu yo'riqnoma talablari buzilganligi haqidagi har qanday faktlar to'g'risida xabar berish, shuningdek, qayd etilgan noutbukning yo'qolishi (o'g'irlanishi) faktlari haqida xabar berish;

noutbukning jismoniy xavfsizligini ta'minlash;

qayd etilgan noutbuklarini boshqa shaxslarga bermaslik.

13. Bank xodimlariga qayd etilgan noutbuklaridan foydalanishda, agar ularning jismoniy xavfsizligini ta’minlash choralari ko‘rilmasa, ularni qarovsiz qoldirish taqiqlanadi.

14. Qayd etilgan noutbuklari bankdan tashqarida (xizmat safarlari, uchrashuvlar, muzokaralar va h.k.) foydalanilganda ularning axborot va jismoniy xavfsizligini ta’minlash maqsadida quyidagi chora-tadbirlar qo‘llanilishi kerak:

autentifikatsiya vositalaridan foydalangan holda qurilmaga kirish uchun parol o'rnatish;

qurilmada virusga qarshi himoya va shaxsiy tarmoqlararo ekran o'rnatish va foydalanish.

15. Qayd etilgan noutbuklarida ushbu yo‘riqnomada belgilangan axborot xavfsizligi talablarini ta’minlash Axborot texnologiyalari departamenti tomonidan amalga oshiriladi.

IV. Mobil, ma’lumot saqlovchi va tashuvchi qurilmalar vositalaridan foydalanish qoidalari va talablari

16. Bankning bank axborot infratuzilmasida faqat bank mulki bo‘lgan hamda Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan muntazam audit va nazoratdan o‘tkaziladigan ro‘yxatdan o‘tgan ma’lumotlar disklari va olinadigan saqlash vositalaridan foydalanishga ruxsat etiladi.

17. Bank xodimlari o'zlarining rasmiy ma'lumotlarini saqlash uchun o'zlarining tashuvchi vositalaridan foydalanishlari mumkin. Shu bilan birga, ularda bankning har qanday konfidensial ma’lumotlarini bankdan tashqarida saqlash yoki olib chiqish uchun foydalanish taqiqlanadi. Ushbu talabni bajarish uchun javobgarlik to'liq bank xodimiga yuklanadi va uning mehnat majburiyatlarida ko'rsatilgan.

18. Bank axborot tizimlari ma’lumotlarini arxivlash – zaxira nusxalarini va elektron arxivlarni saqlash uchun foydalaniladigan DVD va olinadigan qattiq disklar ko‘rinishidagi tashuvchilar Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan hisobga olinadi.

Saqlash tashuvchilari Xavfsizlik va axborotlarni muhofaza qilish departamentining himoyalangan shkaflarida, ularning zaxira nusxalari esa bank obyektlaridan birining hududiy jihatdan olisda joylashgan xavfsiz joyida saqlanadi.

19. Bankda konfidensial ma’lumotlarga ega zaxira nusxalari va elektron arxivlarni saqlash uchun foydalaniladigan qayd etish hisobi olinadigan tashuvchilar maxsus jurnalda hisobga olinadi, uning shakli ushbu yo‘riqnomaning 1-ilovasida belgilangan.

20. Qayd etib, hisobi olib boriladigan ma’lumot saqlovchi va tashuvchi qurilmalar vaqti-vaqti bilan kamida oyiga bir marta virusga qarshi vositalar tomonidan zararli dasturlarga tekshirilishi kerak.

21. konfidensial ma'lumotlarga ega bo'lgan olinadigan tashuvchilarni nazorat qilinadigan hududdan tashqariga olib chiqish faqat bank Xavfsizlik va axborotlarni muhofaza qilish departamenti direktorining ruxsati bilan amalga oshiriladi. Konfidensial ma'lumotlarga tashuvchi qurilmalar tashqariga olib chiqilganda olib tashlash to'g'risidagi ma'lumotlarni qayd etish maxsus jurnalda qayd etiladi (yo'riqnomaning 2-ilovasida keltirilgan namuna asosida).

22. Konfidensial ma'lumotlar bo'lgan zaxira ma'lumotlarini saqlaydigan tashuvchisi nakleyka (stiker) bilan belgilanishi kerak.

Konfidensial ma'lumotlarni o'z ichiga olgan barcha etiketli saqlanadigan tashuvchi axborot vositalari Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan inventarizatsiya qilinishi kerak. Axborot vositalarini va ulardagi belgilar mavjudligini tekshirish Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan yiliga kamida bir marta amalga oshiriladi.

23. Qayd etish hisobi saqlanadigan vositalardan foydalanganda quyidagi talablarga rioya qilish kerak:

ulardan maqsadli foydalanish;

Xavfsizlik va axborotlarni muhofaza qilish departamenti direktorini ushbu yo'riqnoma talablari buzilganligi to'g'risida xabardor qilish, shuningdek, ma'lumot saqlovchi va tashuvchi qurilmalarning yo'qolishi (o'g'irlanishi) yoki ishdan chiqishi faktlari to'g'risida xabardor qilish;

axborot tashuvchilarni boshqa shaxslarga bermaslik.

24. Qayd etish hisobga olinadigan saqlanadigan vositalardan foydalanganda, agar ularning jismoniy xavfsizligini ta'minlash choralari ko'rilmasa, ularni qarovsiz qoldirish taqiqlanadi.

V. Vositalarni hisobdan chiqarish va yo'q qilish tartibi

25. Ishdan chiqqan yoki yo'q qilinishi kerak bo'lgan axborot vositalari, qurilmalar va disklar, shu jumladan konfidensial ma'lumotlar mavjud bo'lganlari, qulflangan metall shkaflar yoki seyflarda saqlanishi kerak.

26. noutbuklari, saqlanadigan tashuvchilar va boshqa shunga o'xshash qurilmalar foydalanishdan chiqarish to'g'risida qaror qabul qilingandan so'ng, ularni yo'q qilish (utilizatsiya qilish) tartibi asosida dalolatnoma tuzish bilan amalga oshirilishi kerak.

27. Foydalanish uchun yaroqsiz qurilmalar, ma'lumot saqlovchi va tashuvchi qurilmalar utilizatsiya qilishda ular ma'lumotlarni o'chirish va saqlash vositalarini formatlash yoki jismoniy yo'q qilish orqali ma'lumotlarni tozalashga beriladi. Konfidensial ma'lumotlarni saqlash uchun foydalanilgan qurilmalarni jismoniy yo'q qilish undan qolgan ma'lumotlarni o'qishga imkon bermasligi kerak, buning uchun barcha mikrosxemalarni bolg'a bilan yo'q qilish kerak.

28. Konfidensial ma'lumotlarga ega bo'lgan saqlanadigan tashuvchilar va ma'lumotlar disklarini utilizatsiya qilish (yo'q qilish) to'g'risidagi ma'lumotlar maxsus jurnalda qayd etiladi, uning shakli ushbu yo'riqnomaning 3-ilovasida keltirilgan.

29. Qurilmalar, boshqa maqsadlarda foydalanishga qaror qilganda, ushbu qurilmalarda saqlangan ma'lumotlar barcha ma'lumotlarni o'chirish, ma'lumotlarni tashuvchi vositalari va saqlash vositalarini formatlash orqali yo'q qilinishi kerak.

30. Agar ma'lumot saqlovchi va tashuvchi qurilmalardan konfidensial ma'lumotlarni o'chirish zarur bo'lsa, ma'lumotni kafolatlangan yo'q qilish vositalaridan foydalanish yoki ushbu vositalarga ega bo'lgan ixtisoslashgan tashkilotlarning xizmatlaridan foydalanish kerak.

VI. Javobgarlik

31. Ushbu yo‘riqnomani buzganlik uchun bank xodimlari shaxsan javobgardirlar.

32. Ushbu yo‘riqnomada belgilangan qoidalarini buzish ichki mehnat qoidalari va O’zbekiston Respublikasining mehnat qonunchiligiga muvofiq intizomiy javobgarlikka tortishga sabab bo‘ladi.

33. Xavfsizlik va axborotlarni muhofaza qilish departamenti ushbu yo‘riqnoma talablarini bajarish uchun javobgardir.

Mobil, ma’lumot saqlovchi va tashuvchi
qurilmalar bilan ishlashda
axborot xavfsizligini ta’minlash bo’yicha
yo’riqnomaga
1-ilova.

Konfidensial ma’lumotlarni tashuvchi vositalarni ro’yxatga olish jurnali

Sana, qurilmaning inventar raqami	Konfidensial ma’lumot tashuvchi tashqi qurilmalar turi (CD, DVD disklar, USB-tashuvchi qurilmalar va boshqalar), xotira xajmi, nomi va ishlab chiqarilgan raqami	Konfidensial ma’lumot tashuvchi tashqi qurilmani qabul qilinganlikni tasdiqlash (F.I.Sh., imzo, sana)	Konfidensial ma’lumot tashuvchi tashqi qurilmani qaytarilganlikni tasdiqlash (F.I.Sh. va ish yurituvchining imzosi, sana)	Konfidensial ma’lumot tashuvchi tashqi qurilmalarni saqlash joyi (seyf, shkaf, javon)	Konfidensial ma’lumot tashuvchi tashqi qurilmalarni yo’q qilinganlikni belgilash (mas’ul xodimning imzosi, sanasi)	Izoh

Mobil, ma’lumot saqlovchi va tashuvchi
qurilmalar bilan ishlashda
axborot xavfsizligini ta’minlash bo’yicha
yo’riqnomaga
2-ilova.

Konfidensial ma’lumot tashuvchi tashqi vositalarni tashqaridan olib kirish hamda tashqariga olib chiqishni ro’yxatga olish jurnali

T/r.	Sana, qurilmaning inventar raqami	Konfidensial ma’lumot tashuvchi tashqi qurilmalar turi (CD, DVD disklar, USB-tashuvchi qurilmalar va boshqalar), xotira xajmi, nomi va ishlab chiqarilgan raqami	Konfidensial ma’lumot tashuvchi tashqi vositani tashqaridan olib kirgan shaxs (F.I.Sh., imzo, sana)	Konfidensial ma’lumot tashuvchi tashqi vositani tashqariga olib chiqqan shaxs (F.I.Sh., imzo, sana)	Izoh

Mobil, ma’lumot saqlovchi va tashuvchi
qurilmalar bilan ishlashda
axborot xavfsizligini ta’minlash bo’yicha
yo’riqnomaga
3-ilova.

Konfidensial ma’lumot tashuvchi tashqi vositalarni yo’q qilish jurnali

T/r.	Sana, qurilmaning inventar raqami	Konfidensial ma’lumot tashuvchi tashqi qurilmalarni turi (CD, DVD disklar, USB-tashuvchi qurilmalar va boshqalar), xotira xajmi, nomi va ishlab chiqarilgan raqami	Konfidensial ma’lumot tashuvchi tashqi vositalarni yo’q qilish (F.I.Sh., imzo, sana)	Konfidensial ma’lumot tashuvchi tashqi vositadan ma’lumotni o’qishga imkon berilmaslik maqsadida qurilmaning barcha mikrosxemalarni jismoniy yo’li bilan (bolg’a yordamida) yo’q qilinishi (F.I.Sh., imzosi, sana)	Konfidensial ma’lumot tashuvchi tashqi qurilmalarni saqlash joyi (seyf, shkaf, javon)	Konfidensial ma’lumot tashuvchi tashqi qurilmalarni yo’q qilinganlikni belgilash (mas’ul xodimning imzosi, sanasi)	Izoh

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
10-ilova

Axborot manbalariga kirish matritsasini ishlab chiqish qoidalari

I. Umumiy qoidalar

1. Ushbu Qoidalar “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank) axborot resurslariga kirish matritsasini (keyingi o‘rinlarda - Kirish matritsasi deb yuritiladi) ishlab chiqish tartibini tavsiflaydi.

Mazkur qoidalarning talablari bankka tegishli axborot resurslari uchun majburiydir.

2. Axborot resurslaridan foydalanishni cheklash qoidalari (foydalanish siyosati) kirish matritsasida shakllantirilgan bo‘lib, unda qaysi subyektlarga (subyektlar guruhlariga), qaysi obyektlarga (obyektlar guruhlariga) kirish huquqlariga (o‘qish, yozish, ijro etish va boshqalar) ruxsat berilgan yoki taqiqlangan.

3. Xavfsizlik va axborotlarni muhofaza qilish departamenti hamda uning axborotni himoya qilish tarkibiy bo‘linmalari Axborot texnologiyalari departamenti bilan birgalikda bank manfaatdor tarkibiy bo‘linmalari rahbarlari bilan kelishilgan holda axborot resurslariga kirish matritsasi ishlab chiqiladi. (ABT uchun administrator buxgalteriya hisobi va moliyaviy menejment departamenti)

4. Kirish matritsasi bank axborot resurslariga kirish huquqiga ega bo‘lgan foydalanuvchilar toifasini, shuningdek, ularning axborotga kirish va qayta ishlash bo‘yicha huquq va vakolatlarini belgilaydi.

Kirish matritsasi foydalanuvchilarning axborot resurslariga kirishini boshqarish uchun ishlatiladi.

5. Foydalanuvchilar toifalari – bu bank xodimlarining funksional vazifalari, faoliyat turi, bajargan ishlari, lavozimi va boshqalar bo‘yicha qo‘shma guruhi.

6. Kirish matritsasi Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoyasi qilish boshqarmasi xodimlari, Active Directory tizimi administratori va Axborot texnologiyalari departamenti xodimlari bo'lgan axborot tizimlari administratorlari tomonidan amalga oshiriladi (ABT uchun administratori Buxgalteriya hisobi va moliyaviy menejment departamenti), korporativ va lokal tarmoqda foydalanishni boshqarish vositalarini hamda axborot tizimlarida ular tomonidan taqdim etilgan kirish identifikatorlari (loginlar, parollar, ERI va boshqalar) asosida foydalanuvchilarni autentifikatsiya qilish va avtorizatsiya qilish vositalarini qo‘llash va boshqarish orqali.

7. Kirish matritsasini tuzishda O‘zbekiston Respublikasi Markaziy banki Boshqaruvining 2020-yil 25-yanvardagi 2/4-son qarori bilan tasdiqlangan O‘zbekiston Respublikasi tijorat Banklarining avtomatlashtirilgan tizimlarida axborotni himoya qilish to‘g‘risidagi nizom talablari amal qiladi shuningdek, O'zbekiston Respublikasi davlat standartlarida axborot xavfsizligini ta'minlash talablari hisobga olinishi kerak.

II. Atamalar va ta’riflar

8. Ushbu qoidalarda quyidagi atamalar va ularning ta’riflari qo‘llaniladi:

1) **kirish huquqi** - obyektga uning vakolati doirasida kirish huquqini beradigan ruxsat;

2) **kirish matritsasi** - foydalanishni boshqarish huquqlarini ko‘rsatadigan jadval.

III. Kirish matritsasini ishlab chiqish uchun talablar

9. Bank axborot tizimlarining axborot resurslariga (ma’lumotlar bazalariga) kirish matritsasi texnik topshiriq va axborot tizimlarini yaratish yoki modernizatsiya qilishga qo‘yiladigan talablarda belgilanadi va axborot tizimlarini qo‘llash dasturini ishlab chiqishda amalga oshiriladi.

10. Axborot tizimlariga kirmaydigan axborot resurslariga bank xodimlarining ko'rsatilgan axborot resurslari ma'lumotlariga (fayl-serverlar, qurilmalar, xizmatlar, web-resurslar va alohida ma’lumotlar bazalari) kirish matritsasi Xavfsizlik va axborotlarni muhofaza qilish departamenti va Axborot texnologiyalari departamenti bilan birgalikda foydalanish darajasidan kelib chiqqan holda ishlab chiqiladi.

Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotni himoyasi qilish boshqarmasi kirish matritsasi ta'rifi talab qilinadigan ko'rsatilgan axborot resurslari ro'yxatini yuritishi kerak.

11. Axborot resurslaridan foydalanish matritsasini ishlab chiqish quyidagi tartibda amalga oshiriladi:

1) Bankning kirish nazorat qilinishi kerak bo‘lgan axborot resurslari ro‘yxati shakllantiriladi;

2) har bir axborot resursi uchun unga kirish huquqiga ega bo‘lgan foydalanuvchilar ro‘yxati shakllantiriladi;

3) foydalanuvchilar ro'yxati egallab turgan lavozimi, funksional majburiyatlari va xodimlarning vakolatlarini hisobga olgan holda, ularning huquqlari va kirish ruxsatlarini ko'rsatgan holda foydalanuvchilar toifalariga bo'linadi;

4) axborot resurslariga kirish uchun ruxsat olish tartiblarini belgilash va amalga oshirish.

12. Har bir axborot resursi uchun alohida kirish matritsasi quyidagilarni o'z ichiga olishi kerak:

1) unga kirish huquqiga ega bo'lgan foydalanuvchilar ro'yxati;

2) ularning huquqlari va foydalanish huquqlarini ko'rsatadigan foydalanuvchilar toifalari ro'yxati;

3) kirish uchun ruxsat olish tartiblari.

13. Foydalanuvchilar toifalarini aniqlashda xodimlarning lavozimi, funksional majburiyatlari va vakolatlari hisobga olinadi.

Individual axborot resurslari uchun kirish matritsasi ularga berilgan huquqlarga muvofiq ma’lum bir foydalanuvchi uchun axborot manbasiga kirish jadvalini (belgilangan vaqt orasida axborot manbasiga kirish) ko‘rsatishi mumkin.

14. Axborot resurslaridan foydalanuvchilarga quyidagi huquqlar va vakolatlar berilishi mumkin:

Read (R) - obyektdan ma’lumot olish;
Write (W) - obyektdagi ma’lumotlarni yangilash;
Append (A) - obyektga yangi ma’lumotlar qo‘shish;
Execute (Y) - obyektni bajariladigan kod sifatida talqin qilish;
Delete (D) – obyektni o‘chirish;
Get info (G) - obyekt haqida ma’lumot olish;
Set info (S) - obyekt haqida ma’lumot o‘rnatish;
Privilege (P) - obyektga kirish huquqlarini sozlash.

15. Kirish matritsasini ishlab chiqishda quyidagi talablarni hisobga olish kerak:

muayyan sharoitlarda qo’llaniladigan majburiy va tavsiya etilgan qoidalar o’rtasidagi farqlar;

“Taqiqlanmaguncha hamma narsaga ruxsat beriladi” degan zaif tamoyil asosida emas, balki “hamma narsaga aniq ruxsat berilmaguncha umuman taqiqlanishi kerak” mazmundagi tamoyilga asoslanib qoidalarni shakllantirish;

axborotni qayta ishlash vositalari tomonidan avtomatik ravishda hosil qilinadigan va foydalanuvchilarning ixtiyoriga binoan boshlangan ma’lumotlarning konfidensiallik darajasidagi o’zgarishlar;

axborot tizimi tomonidan avtomatik ravishda o’rnatiladigan va administrator tomonidan belgilanadigan foydalanuvchi huquqlarining o’zgarishi;

kuchga kirgunga qadar maxsus tasdiqlashni talab qiladigan va talab qilmaydigan qoidalar.

16. Ishlab chiqilgan kirish matritsasi bankning manfaatdor tarkibiy bo‘linmalari bilan kelishilgan va bank rahbariyati tomonidan tasdiqlangan.

17. Kirish matritsasi asosida bank xodimlariga berilgan huquq va rollarga muvofiq axborot resurslariga kirishni chegaralash va boshqarish tizimlari joriy etiladi.

18. Axborot resurslariga kirishda axborotni qayta ishlashning yangi vositalaridan foydalanishga ruxsat olish uchun quyidagi harakatlar bajarilishi kerak:

yangi vositalar va ularning maqsadi rahbariyat tomonidan tasdiqlanishi va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori bilan kelishilishi kerak;

joriy etishdan oldin dasturiy ta'minot va texnik vositalarning tizimning boshqa komponentlari bilan muvofiqligini tekshirish zarur;

ish joyida rasmiy ma'lumotlarni qayta ishlash uchun shaxsiy texnik axborotlashtirish vositalaridan (masalan, noutbuklar, uy kompyuterlari va boshqalar) foydalanish taqiqlanishi kerak.

19. Asosiy axborot manbalariga kirish matritsasi bankning ushbu qoidalarga ilovada tarzida keltirilgan. Bank Axborot xavfsizligi siyosatiga ilova qilingan alohida faylda yuritiladi.

Axborot manbalariga kirish
matritsasini ishlab chiqish
qoidalariga ilova

“O‘zsanoatqurilishbank” ATBning axborot resurslariga kirish matritsasi

Foydalanuvchilar	ABS	CRM tizimi	DWH тизими	CROBS tizimi	ELMA BPM tizimi	ЭДО tizimi	SAP Basis tizimi	SWIFT tizimi	Way4 protsessing tizimi	Internet-banking	Mobilnыy banking	Bosh bank fayl-server	HBXM va BXM fayl-serveri	Veb-sayt Intranet	Rasmiy web-sayt
Bosh bank															
Rahbariyat															
Boshqaruv Raisi															
Boshqaruv Raisining birinchi o’rinbosari															
Boshqaruv Raisi o’rinbosari															
Boshqaruv Raisi o’rinbosari															
Boshqaruv Raisi o’rinbosari															
Boshqaruv Raisi o’rinbosari															
Boshqaruv Raisi o’rinbosari															
Moliyaviy resurslarni boshqarish bosh direktori															
Kredit bosh direktori															
Risk bosh direktori															
Rahbariyat qoshida															
Boshqaruv Raisi maslahatchisi															
Korporativ boshqaruv xizmati															
Korporativ maslahatchi															
korporativ boshqaruv xizmati rahbari															
korporativ boshqaruv xizmati rahbari o’rinbosari															
korporativ boshqaruv xizmati rahbari o’rinbosari															
yetakchi mutaxassis															
Axborot xizmati															
Axborot xizmati rahbari-Boshqaruv Raisining axborot siyosati bo’yicha maslahatchisi															
menejer															
……															

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
11-ilova

Foydalanish uchun ruxsat etilgan dasturiy ta’minot ro‘yxati

I. Umumiy qoidalar

1. Ushbu hujjat “O‘zsanoatqurilishbank” ATB xodimlari tomonidan ish stansiyalari va serverlarda foydalanishga ruxsat berilgan dasturiy ta’minotdan foydalanishga qo‘yiladigan talablarni belgilaydi hamda ushbu talabni bajarish tartibini belgilaydi.

2. Ushbu hujjatning dasturiy ta’minotni o‘rnatishni cheklash bo‘yicha talablari Bankda foydalaniladigan barcha ish stansiyalari va serverlariga nisbatan bajarilishi kerak.

3. Bank xodimlarining ish joylari o‘zlarining xizmat vazifalarini bajarishlari uchun zarur bo‘lgan va Bankda foydalanish uchun tasdiqlangan dasturiy ta’minotni o‘rnatishlari shart.

Bank xodimlarining muayyan toifasiga nisbatan qo‘shimcha ixtisoslashtirilgan dasturiy ta’minotdan foydalanishga ruxsat berilishi mumkin.

Serverlarga ularning ishlashi va xizmat ko'rsatish yoki axborot tizimini tashkil qilish uchun zarur bo'lgan dasturiy ta'minot o'rnatilgan bo'lishi kerak.

4. Dasturiy ta'minotdagi mumkin bo'lgan zaifliklarni, ma'lumotlarning sizib chiqishi kanallarini kamaytirish, noma'lum dasturlar yoki ishonchli bo'lmagan dasturlarni o'rnatishni istisno qilish, shuningdek, keraksiz dasturlar tomonidan ma'lumotlarni qayta ishlash vositalarini haddan tashqari yuklab olishni istisno qilish uchun dasturiy ta'minotdan foydalanishga nisbatan cheklovchi talablar kiritilgan.

II. Dasturiy ta'minotdan foydalanishga qo'yiladigan talablar

5. Operatsion tizim va uning komponentlarini, ish stansiyalari va serverlarida dasturiy ta'minotni o'rnatish va yangilash Axborot texnologiyalari departamenti va MBXOdagi Axborot texnologiyalari bo'limlari tomonidan amalga oshiriladi.

6. Bank xodimlari tomonidan ish stansiyalarida operatsion tizim va dasturiy ta’minotni o‘zboshimchalik bilan o‘rnatishga yo‘l qo‘yilmaydi.

7. Bank xodimlarining ish joylarida foydalanuvchi huquqlari o‘rnatiladi.

8. Administrator huquqlari, agar kerak bo'lsa (serverlar va jihozlarga xizmat ko'rsatish uchun foydalaniladi) administratorning alohida ish stansiyalarida axborot texnologiyalari departamenti direktorining ruxsati bilan o'rnatiladi.

9. Foydalanishga ruxsat berilgan dasturiy ta'minotlar ro'yxati jadvalda keltirilgan.

Foydalanish uchun ruxsat etilgan dasturiy ta’minot ro‘yxati

1. Ish stansiyalarida o'rnatilgan dasturlar	
1. Operatsion tizimlar	
1.1.	Microsoft Windowsdan 7, 8, 10, 11 operatsion tizimlari, shu jumladan ularning yangilanishlari (muhim, xavfsizlik, funksionallikni yaxshilash va dasturlardagi xatolarni bartaraf etish)
2. Ofis dasturlari	
2.1.	Microsoft Office 2008, 2010, 2013, 2016, 2019 oilasining ofis dasturlari.
3. Uchinchi tomon axborot tizimlarining dasturiy mahsulotlari	
3.1.	“Norma” axborot-qidiruv tizimi
4. Elektron pochta	
4.1.	Microsoft Outlook
5. Elektron hujjat aylanishi	
5.1.	Elektron hujjat aylanish tizimi dasturi "Fido-Business" tomonidan ishlab chiqilgan
5.2.	LotusNotes
5.3.	EXAT himoyalangan elektron pochta
6. Axborotni shifrlash va deshifrlash uchun dasturiy mahsulotlar	
6.1.	Connection Manager Client, Agro Crypt, SFiT Client, Styx Client, OpenVPN
7. Antivirus dasturi	
7.1.	Kaspersky antivirus mahsuloti
7.2.	Viruslarni yo'q qilish vositalari
8. Fayl menejerlari	
8.1.	Total Commander
8.2.	FarManager, WinSCP
9. Arxivlash	
9.1.	Arj, Rar, Zip
10. Pdf fayllar bilan ishlash uchun dasturlar	
10.1.	Faylni ko'ruvchi dasturlar PDF: Adobe Acrobat reader, Foxit Reader, ABBYY FineReader
10.2.	Fayl tahrirlash dasturlari PDF: AdobeProfessional, NitroPro, ABBYY FineReader
11. Video va audio pleyerlar, foto tahrirlash	
11.1.	Windows Media Player, AIMP, Pot player, X Codec Pack, Photoshop, Corel Draw, ACD, K-Lite Codec Pack
12. USB- xavfsizlik belgisi	
12.1.	SafeNetIkey 1000, RainbowiKey 100, Styx Toc
13. Maxsus dasturiy ta'minot	
13.1	PLSQL developer, Intellij Idea, Visual Studio Code, PhpStorm, DBeaver, Docker, Postman, Insomnia, virtualizatsiya tizimi, Nextcloud, NetLimiter, ma'lumotlarni yozib olish vositalari CD va Flash tashuvchilar, Zoom, Punto Switcher, Java, Putty, PO SAP (SAP Analysis, SAP Logon, SAP HANA studio), Vmware (virtualizatsiya tizimi), Windows Power Shell, WinSCP, Xming, Eclipse, Jenkins.
14. Internet - brouzerlar	
14.1.	Google Chrome, Mozilla FireFox, Internet Explorer, Microsoft Edge
15. Drayverlar va utilit dasturlari	
15.1.	Kompaniya tomonidan ishlab chiqarilgan dasturlar va utilit dasturlar Sun
15.2.	Kompaniya tomonidan ishlab chiqarilgan dasturlar va utilit dasturlar Microsoft
16. O'z rivojlanishi uchun axborot tizimlarining dasturiy mahsulotlari	
16.1.	Dasturiy ta'minot kompleksi ABT
16.2.	Dasturiy ta'minot kompleksi ОДБ NBS+PAYMENT

16.3.	Dasturiy ta'minot kompleksi I-BANK
16.4.	Interaktiv axborot tizimi “Personal”
2. Serverlarda o'rnatilgan dasturlar	
1. Operatsion tizimlar	
1.1.	Microsoft tomonidan Windows Server 2008, 2012, 2016 oilasining operatsion tizimlari, shu jumladan ularning yangilanishlari (muhim, xavfsizlik, funksionallikni yaxshilash va dasturlardagi xatolarni bartaraf etish)
1.2.	operatsion tizimlari Linux (Centos 7-8, Oracle 7-8, Ubuntu 18-20, SUSE) va Unix, ularning yangilanishlari.
2. MBBT	
2.1.	Oracle, PostgreSQL, SAP HANA, SYBASE, MS SQL
2. Antivirus dasturi	
2.1.	Kaspersky antivirus mahsuloti
3. Arxivlash	
3.1	Rar, Zip.
4. Internet brauzerlar	
4.1	Google Chrome, Mozilla FireFox.
5. Fayl menejerlari	
5.1.	Total Commander, Midnight Commander.
6. Maxsus dasturiy ta'minot	
6.1	SAP BW/4HANA, SAP Web Dispatcher, SAP Diagnostic Agent, SAP Solution Manager, SAP BussinesObject, SAP Lumira Server, SAP Router, Komponentlar DT «Cash Management», Komponentlar DT «SUO и SOKOK», Komponentlar DT «Collection».

10. Ixtisoslashtirilgan vazifalarni bajarish uchun zarur bo'lgan alohida ish stansiyalarida qo'shimcha dasturiy ta'minotni o'rnatish Axborot texnologiyalari departamenti direktori va Xavfsizlik va axborotlarni muhofaza qilish departamenti bilan kelishilganidan keyin amalga oshiriladi.

11. Ishlab chiquvchilar yangilanishlar yoki dasturlarni qo'llab-quvvatlashni to'xtatgan, shuningdek, funksional jihatdan ustunroq bo'lgan yoki ro'yxatda ko'rsatilganidan arzonroq bo'lgan yangi dasturlar paydo bo'lgan hollarda boshqa shunga o'xshash dasturiy ta'minotdan foydalanishga ruxsat beriladi. Shunga o'xshash dasturiy ta'minotdan foydalanish Axborot texnologiyalari departamenti direktori va Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan tasdiqlanishi kerak.

12. Foydalanishga ruxsat etilgan dasturiy ta’minotlar Ro‘yxatiga o‘zgartirish va qo‘shimchalar Axborot texnologiyalari departamenti direktori va Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan kiritilishi, so‘ngra bank rahbariyati tomonidan tasdiqlanishi mumkin.

13. Bankda ruxsat etilmagan dasturiy ta’minotdan foydalanish holatlarini aniqlash maqsadida Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimlari tomonidan ish stansiyalari va boshqa so‘nggi qurilmalarni tanlab yoki to‘liq tekshirish ishlari olib borilmoqda. Tasdiqlanmagan dasturiy ta'minotdan foydalanishda buzilishlar aniqlangan taqdirda, aybdorga nisbatan intizomiy jazo choralari qo'llanilishi mumkin.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
12-ilova

Internet va korporativ elektron pochta bilan ishlash bo‘yicha yo’riqnoma

I. Umumiy qoidalar

1. Ushbu yo‘riqnoma “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank) xodimlarining internet tarmog‘idan foydalanish va elektron pochta bilan ishlash tartibi va talablarini belgilaydi.

2. Bank xodimlariga bank korporativ tarmog‘ini asosiy va zaxiraviy ma’lumotlarni qayta ishlash markazlarida tashqi internet tarmog‘iga ulash chegarasida o‘rnatilgan proksi-serverlar orqali internet tarmog‘idan markazlashtirilgan holda foydalanish ta’minlanadi.

3. Internetga kirish o'zlarining rasmiy vazifalarini bajarish uchun bunday kirishni talab qiladigan Bosh ofis va ABning ayrim xodimlariga taqdim etiladi.

4. Bank xodimlariga internet tarmog‘iga kirish bank rahbariyatiga tuzilmaviy bo‘linma rahbari nomidan kiritilgan ariza asosida taqdim etiladi.

Internetga kirishni ta'minlash uchun arizada quyidagilar ko'rsatilgan:

bank xodimining to'liq ismi, lavozimi va Internet-resurslar bilan ishlash zarurati asoslari.

bank rahbariyati tomonidan ma’qullangandan so‘ng ariza Xavfsizlik va axborotlarni muhofaza qilish departamentiga yuboriladi.

bank rahbariyatining roziligisiz mustaqil ravishda tashkil etish va bank xodimlariga Internet tarmog‘iga kirishni ta’minlash taqiqlanadi.

5. Internet tarmog'iga kirishni ta'minlashdan oldin bank xodimi ushbu Yo'riqnoma bilan tanishishi, shuningdek, Internetdan foydalanish bo'yicha ushbu Yo'riqnomada belgilangan talablarga rioya qilish majburiyatini imzolashi kerak.

6. Bank xodimining internet tarmog‘iga kirishi Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoya qilish boshqarmasi proksi-serverlarga xizmat ko‘rsatuvchi mas’ul xodimi tomonidan ta’minlanadi.

Ushbu xodim Internet foydalanuvchilari jurnalini ham yuritadi, unda quyidagilar qayd etiladi:

ro'yxatga olingan sana;

F.I.SH. va bank xodimining lavozimi;

bankning tarkibiy bo'linmasining nomi;

ro'yxatdan o'tish uchun asoslar (ariza raqami va sanasi).

7. Xodimning Internetga kirishi uning ish joyidan amalga oshiriladi. Boshqa shaxsning ish stansiyasidagi xatti-harakatlari uchun javobgarlik ushbu harakat amalga oshirilgan ish stansiyasining foydalanuvchisiga yuklanadi.

8. Bank o‘zining korporativ elektron pochta serverini yaratadi. Korporativ pochta bank xodimiga Internet orqali tashqi foydalanuvchilar bilan elektron pochta xabarlarini almashish imkonini beradi. Korporativ elektron pochtadan foydalanish

huquqi o'z xizmat vazifalarini bajarish uchun ushbu almashinuvga muhtoj bo'lgan alohida bank xodimlariga beriladi.

Bank doirasida pochta xabarlarini almashish uchun bank xodimlari Banklararo elektron pochtadan foydalanadilar.

9. Korporativ elektron pochta bank xodimlariga bankning tarkibiy bo‘linmasi rahbari nomidan bank rahbariyatiga yo‘llangan ariza asosida taqdim etiladi.

Bank xodimining Banklararo elektron pochta tizimiga kirishi bank lokal va korporativ tarmog‘iga ulanganida ishga qabul qilish to‘g‘risidagi buyruq asosida amalga oshiriladi.

Shaxsiy korporativ elektron pochta manzili va/yoki ishga tushirilgan parolga ega Banklararo elektron pochta manzili bank xodimiga telefon orqali yetkaziladi yoki lokal va korporativ tarmoqqa kirish rekvizitlari bilan birga taqdim etiladi.

Xodimlarni korporativ va Banklararo elektron pochtaga ulash Axborot texnologiyalari departamenti tomonidan amalga oshiriladi.

10. Korporativ elektron pochta va Banklararo elektron pochta bank xodimlari va tashqi foydalanuvchilar bilan matnli xabarlar yoki elektron shakldagi hujjatlar ko‘rinishidagi rasmiy ma’lumotlarni almashish uchun ishlatiladi.

Har qanday konfidensial ma'lumotlarni korporativ va Banklararo elektron pochta orqali shifrlanmagan shaklda va elektron raqamli imzo (keyingi o'rinlarda - ERI) dan foydalanmasdan o'tkazish taqiqlanadi, ya'ni. uning konfidensialligi va yaxlitligini ta'minlamasdan.

11. Tashqi messenjerlardan (tezkor xabar almashish tizimlari) foydalanish huquqi o'z xizmat vazifalarini bajarish uchun bunday ruxsatga muhtoj bo'lgan bank xodimlariga beriladi. Ushbu xodimlarning ro‘yxati bank rahbariyati tomonidan belgilanadi yoki bankning tarkibiy bo‘linmasi rahbari nomidan bank rahbariyatiga yo‘llangan ariza asosida taqdim etiladi.

12. Konfidensial ma’lumotlarni tezkor xabar almashish tizimlari, shuningdek, Internet tarmog‘idagi boshqa axborot almashish tizimlari (Internet pochtasi, ijtimoiy tarmoqlar, onlayn videokonferensiyalar va boshqalar) orqali o‘tkazish taqiqlanadi.

13. Internetdan va elektron pochta orqali olingan har qanday elektron ma'lumot virusga qarshi himoya vositalaridan foydalangan holda zararli dastur mavjudligi bo’yicha tekshirilishi kerak.

II. Internet foydalanuvchilari uchun asosiy talablar

14. Bank xodimlarining internet tarmog‘iga kirishini tashkil etishda ularni bank korporativ tarmog‘ini tashqi internet tarmog‘iga ulash chegarasida o‘rnatilgan proksi-server orqali ulanishi talabiga rioya qilish kerak..

15. Internetdan foydalanganda quyidagilarga rioya qilinishi kerak:

ushbu yo'riqnoma talablariga rioya qilish;

internetdan faqat o'z xizmat vazifalarini bajarish uchun foydalanish;

bank xavfsizligi departamenti xodimlarini ushbu yo'riqnoma talablari buzilganligi to'g'risida har qanday faktlar to'g'risida xabardor qilish.

16. Bank xodimlari Internetdan quyidagi maqsadlarda foydalanish huquqiga ega:

bank faoliyati va u ko‘rsatayotgan bank xizmatlari to‘g‘risida hamma uchun

ochiq ma’lumotlarni tarqatish;

bankning yangiliklar ma’lumotlarini Internet tarmog‘ida, shuningdek, bankning ommaviy tadbirlari haqidagi ma’lumotlarni yoritish;

bank mijozlari bilan o‘zaro hamkorlik va munosabatlarni amalga oshirish, ularni Bankdan bank xizmatlarini olish tartibi va qoidalari bilan tanishtirish;

O‘zbekistonning ijtimoiy-siyosiy va ijtimoiy-iqtisodiy hayoti bilan tanishish hamda respublika va jahonda ro‘y berayotgan so‘nggi voqealar haqida ma’lumot olish;

bank sohasida marketing tadqiqotlarini o'tkazish, ichki bank bozorini o'rganish;

bankning rasmiy web-saytini yuritish va uni o‘z vaqtida dolzarb ma’lumotlar bilan to‘ldirish;

bank xodimlari tomonidan o‘z faoliyatini amalga oshirish uchun zarur bo‘lgan ma’lumotlarni Internet tarmog‘idagi turli manbalardan olish;

bank sohasida xorijiy tajriba va xalqaro tendensiyalarni o'rganish;

o'zaro hamkorlik va tajriba almashish doirasida xorijiy, xalqaro va milliy tashkilotlar bilan axborot almashish;

bank xodimlari tomonidan onlayn xizmatlardan foydalanish, xususan, chiptalar sotib olish, mehmonxonalarni band qilish, viza olish va h.k.

bank tomonidan xizmat safarlari, xorijiy vakillarni qabul qilish, boshqa tadbirlarni o‘tkazish bilan bog‘liq tashkiliy masalalarni hal etish;

dasturiy ta'minotni o'z vaqtida yangilash va boshqalar.

17. Internetdan foydalanganda quyidagilar taqiqlanadi:

taqdim etilgan Internetdan shaxsiy maqsadlarda yoki ko'ngilochar maqsadlarda foydalanish;

internetga ruxsatsiz kirishni qo'lga kiritish;

konfidensial ma'lumotlarni shifrlanmagan holda uzatish;

xodimlarga internet tarmog‘iga ruxsatsiz kirish imkonini beruvchi maxsus apparat va dasturiy ta’minotlardan foydalanish;

bank tarmoq infratuzilmasi elementlarining normal ishlashini buzishga qaratilgan har qanday harakatlarni amalga oshirish;

ish stansiyalarini ruxsatsiz ochish va o'rnatilgan operatsion tizimning apparat va dasturiy ta'minot konfiguratsiyasi va parametrlariga o'zgartirishlar kiritish;

tarmoq kabelini mexanik stressga duchor qilish va ish stansiyasi va periferik qurilmalarni fizik, issiqlik va kimyoviy ta'sirlarga duchor qilish;

Axborot texnologiyalari departamenti ruxsatisiz ish stansiyasiga, lokal va korporativ qo‘shimcha uskunalar tarmog‘iga ruxsatsiz ulanish;

ish stansiyasida ruxsatsiz kirish va virusga qarshi dasturlardan himoya qilish ishlarini blokirovka qilish;

boshqa birovning qayd ma'lumotlari va ro'yxatdan o'tmagan tarmoq yoki apparat manzilidan foydalanish;

internet tarmog‘iga kirishning boshqa shakllaridan foydalanish, Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan ruxsat etilganlar bundan mustasno, shuningdek, Internet tarmog‘iga anonim kirish uchun turli sayt va dasturlardan foydalanish;

internetda ishlashda tashqi proksi-serverlar, VPN-serverlar, TOR tarmoqlari, peer-to-peer tarmoqlari va anonimatorlardan foydalanish;

bankning har qanday korporativ elektron pochta manzillarini, shu jumladan

e'lonlar taxtalarida, konferensiyalarda va mehmonlar kitoblarida nashr etish;

korporativ bo'lmagan elektron pochta, ijtimoiy tarmoqlar va tashqi tezkor xabar almashish tizimlaridan xususiy va konfidensial ma'lumotlarni jo'natish uchun foydalanish;

foydalanuvchi qayd ma'lumotlari va parollarini uzatish;

katta tarmoq yukini yaratadigan va boshqa foydalanuvchilarning normal ishiga xalaqit beradigan oqimli video eshittirish resurslariga tashrif buyurish;

internet tarmog'ida qonunga, shuningdek ushbu Yo'riqnomaga zid bo'lgan noqonuniy operatsiyalarni amalga oshirish va boshqa harakatlarni amalga oshirish.

18. Bank xodimlari quyidagi huquqlarga ega:

internetga kirish huquqini olish uchun ariza berish;

internet tarmog‘iga kirishga to‘sqinlik qiladigan texnik xatolar aniqlanganda Axborot texnologiyalari departamentiga murojaat qilish;

ushbu yo‘riqnoma talablari buzilganligi to‘g‘risida Xavfsizlik va axborotlarni muhofaza qilish departamentini xabardor qilish;

internet tarmog‘iga kirishda kontentni filtrlash qoidalarini o‘zgartirish bo‘yicha takliflar kiritish;

shaxsiy foydalanish uchun kompyuter texnikasini ajratish va modernizatsiya qilish va ishlash uchun zarur bo'lgan dasturiy ta'minotni o'rnatish uchun arizalar taqdim etish.

III. Internet orqali ma'lumot olish va tarqatish

19. Bank xodimlari ma’lumotlarni olish va tarqatish maqsadida o‘z ish stansiyalari orqali internet tarmog‘iga ulanadi.

20. Bank xodimlari Internet tarmog‘idan o‘z xizmat vazifalarini bajarish uchun zarur bo‘lgan har qanday ma’lumotni internet tarmog‘idagi axborot resurslariga qidiruv tizimlari orqali kirish yoki URL manzilini kiritish orqali olishlari mumkin.

Proksi-server orqali bank xodimlarining ushbu yo‘riqnoma da taqiqlangan va bank Axborot xavfsizligi siyosatiga zid bo‘lgan internet resurslaridan foydalanishiga cheklovlar o‘rnatilishi mumkin.

21. Bank xodimlari quyidagi maqsadlarda Internet tarmog‘ida axborot tarqatish huquqiga ega:

bank, uning tarkibiy bo‘linmalari faoliyati va bank xizmatlari to‘g‘risidagi hamma uchun ochiq ma’lumotlarni yoritish;

bankning ommaviy tadbirlari to‘g‘risidagi axborot va yangiliklarni tarqatish;

bank mijozlariga ularning xizmatlarini ko'rsatish tartibi va qoidalari, shuningdek ularni olish joylari to'g'risida zarur ma'lumotlarni yetkazish;

bankdagi bo‘sh ish o‘rinlari to‘g‘risidagi ma’lumotlarni tarqatish;

bank bilan o‘zaro hamkorlik qilish uchun aloqa ma’lumotlari va boshqa ma’lumotlarni taqdim etish.

22. Yuqoridagi ma’lumotlarni tarqatish huquqi bank xodimlariga o‘z xizmat vazifalariga muvofiq faqat bank rahbariyatidan bunday kontentni tarqatish zarurligi to‘g‘risida olingan ko‘rsatmalarning bajarilishi munosabati bilan beriladi.

23. Internet tarmog‘ida ma’lumotlarni tarqatishda bank xodimlari quyidagi talablarga rioya qilishlari shart:

ishonchli, to'liq va obyektiv axborotni nashr etish;

materiallarni nashr qilishda, shu jumladan shaxsiy fikrni bildirgan holda, faqat o'z xizmat vazifalariga rioya qilish;

nashrlar bank to‘g‘risida fikr va taassurot shakllantirayotganini esda tutish;

iste'molchilar huquqlarini himoya qilish to'g'risidagi qonun hujjatlari talablariga rioya qilish;

nashr etilgan materiallar uchun to'liq javobgarlikni bilish;

uchinchi shaxslarning intellektual faoliyat natijalari va individuallashtirish vositalariga bo'lgan huquqlariga rioya qilish va hurmat qilish;

boshqa Internet foydalanuvchilari bilan ziddiyatlardan, konstruktiv bo'lmagan nizolardan qochish.

24. Quyidagilarni o'z ichiga olgan materiallarni nashr etish, yuklash va tarqatish taqiqlanadi:

konfidensial ma'lumotlar, shuningdek tijorat va bank sirlarini tashkil etuvchi ma'lumotlar, shaxsiy ma'lumotlar, agar ular xizmat vazifalariga kirsa va uzatish usuli xavfsiz bo'lsa, Xavfsizlik va axborotlarni muhofaza qilish departamenti yoki bank rahbariyati bilan kelishilgan hollar bundan mustasno;

egasining ruxsatisiz to'liq yoki qisman mualliflik huquqi yoki boshqa huquqlar bilan himoyalangan axborot;

ruxsatsiz kirish uchun har qanday apparat, dasturiy ta'minot va dasturiy ta'minotning funksionalligini buzish, yo'q qilish yoki cheklash uchun mo'ljallangan zararli dasturiy ta'minot;

tijoriy dasturiy ta'minot va ularni yaratish uchun dasturiy ta'minotning seriya raqamlari, parollar va pullik Internet-resurslarga ruxsatsiz kirishning boshqa vositalari, shuningdek yuqoridagi ma'lumotlarga havolalar;

tahdid soluvchi, tuhmat, behayo mazmundagi ma’lumotlar, shuningdek, boshqa shaxslarning sha’ni va qadr-qimmatini kamsituvchi ma’lumotlar, millatlararo adovatni qo‘zg‘atuvchi, zo‘ravonlikni qo‘zg‘atuvchi, qonunga xilof faoliyatga chaqiruvchi materiallar va qonun hujjatlariga zid bo‘lgan boshqa ma’lumotlar;

boshqa xizmat ma'lumotlari.

25. Internet tarmog‘ida axborot resurslarini tarqatishda Vazirlar Mahkamasining qarori bilan tasdiqlangan O‘zbekiston Respublikasi axborot resurslarini ma’lumotlar tarmoqlarida, shu jumladan Internet tarmog‘ida tayyorlash va tarqatish tartibi to‘g‘risidagi nizom talablari. O‘zbekiston Respublikasining 1999 yil 26 martdagi 137-sonli qarori va O‘zbekiston Respublikasi Vazirlar Mahkamasining 2005 yil 22 noyabrdagi 256 - sonli qarori bilan tasdiqlangan Davlat axborot resurslarini shakllantirish tartibi to‘g‘risidagi nizomga rioya etilishi shart.

26. Internet-resurslarning mazmuni, shuningdek, Internetdan yuklab olingan fayllar zararli dasturlarning yo'qligi uchun majburiy tekshiruvdan o'tkaziladi.

27. Taqiqlanadi:

katta tarmoq yukini yaratadigan va boshqa foydalanuvchilarning normal ishlashiga xalaqit beradigan, shuningdek, Internetdan katta hajmdagi fayllarni (25 MB dan ortiq) jo'natish yoki qabul qiluvchi oqimli video eshittirish resurslariga tashrif buyurish;

erotik-pornografik internet resurslariga, millatchilik tashkilotlarining resurslariga, zo'ravonlik va terrorizmni targ'ib qiluvchi manbalarga tashrif buyurish va ulardan foydalanish;

internet tarmog'ida qonunga, shuningdek ushbu Yo'riqnomaga zid bo'lgan noqonuniy operatsiyalarni amalga oshirish va boshqa harakatlarni amalga oshirish.

28. Xavfsizlik va axborotlarni muhofaza qilish departamenti bank Axborot xavfsizligi siyosatiga zid bo‘lgan va xodimlar faoliyati bilan bog‘liq bo‘lmagan ayrim internet resurslaridan proksi-server bo‘yicha so‘rovlar va trafikni filtrlash orqali xodimlarning kirishini cheklash huquqiga ega.

IV. Internet-resurslardan foydalanish bo‘yicha nazorat

29. Proksi-server orqali Internetga kirishda bank xodimlariga faqat "oq ro'yxat"da belgilangan ruxsat etilgan tashqi resurslardan foydalanish huquqi beriladi.

30. “Oq ro‘yxat” Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan tuziladi va bank rahbariyati bilan kelishiladi.

31. Tashqi internet resurslariga kirishni cheklash va “oq ro‘yxat”ga kiritilgan resurslarga kirishni ta’minlash proksi-server orqali amalga oshiriladi.

32. Kirishni cheklash proksi-serverdagi tarmoq so'rovlari va trafikni filtrlash orqali amalga oshiriladi.

33. Bank foydalanuvchilarning mazmuni xizmat vazifalarini bajarish bilan bog‘liq bo‘lmagan internet-resurslarga, shuningdek mazmuni va yo‘nalishi milliy qonunchilik va xalqaro tashkilotlar tomonidan taqiqlangan resurslarga kirishini bloklash yoki cheklash huquqini o‘zida saqlab qoladi.

34. Xavfsizlik va axborotlarni muhofaza qilish departamenti bank xodimlari tomonidan internet resurslaridan foydalanish hisobini yuritadi, ushbu yo‘riqnoma ga rioya etilishini nazorat qiladi va internet resurslaridan xavfsiz foydalanishni ta’minlaydi.

35. Xavfsizlik va axborotlarni muhofaza qilish departamenti bank xodimlarining ular bilan oldindan kelishilmagan holda internet resurslaridan maqsadli foydalanishini nazorat qilish maqsadida tanlab va to‘liq tekshirishlar o‘tkazishga haqli.

36. Xodimlar foydalanadigan internet-resurslar to‘g‘risidagi ma’lumotlar ularni keyingi tahlil qilish uchun proksi-serverlar tomonidan yuritiladi va zarurat tug‘ilganda, nazorat qilish uchun tarkibiy bo‘linmalar rahbarlariga, shuningdek bank rahbariyatiga taqdim etilishi mumkin.

37. Bank xodimlarining Internet tarmog‘idagi foydalanishini nazorat qiluvchi proksi-serverlar ishining natijalari, shuningdek, Internet tarmog‘idan maqsadli foydalanishni tanlab va to‘liq tekshirish natijalariga ko‘ra ushbu yo‘riqnoma ni eng yomon niyatli buzuvchilar aniqlanadi.

38. Noto'g'ri foydalanish faktlari "Internetdan noto'g'ri foydalanish to'g'risidagi qonun" shaklida qayd etiladi, u Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan tayyorlanadi va uning direktori tomonidan imzolanadi.

Aniqlangan internet tarmog‘idan noto‘g‘ri foydalanish faktiga ko‘ra, yomon niyatli huquqbuzardan tushuntirish xati shaklida yozma ko‘rsatma olinadi.

Internet tarmog‘idan noto‘g‘ri foydalanish to‘g‘risidagi dalolatnoma tegishli choralar ko‘rish uchun Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga taqdim etiladi.

39. Agar xodim Internetdan noto'g'ri foydalanishda gumon qilinsa, ichki audit boshlanadi.

V. Elektron pochtadan foydalanish qoidalari

40. Korporativ va Banklararo elektron pochta bilan ishlashda bank xodimi quyidagi asosiy qoidalarni hisobga olishi kerak:

elektron pochta yuborilgan xabarni qabul qiluvchiga kafolatlangan yetkazib berish vositasi emasligi;

elektron pochta uzatilayotgan ma'lumotlarning konfidensialligini ta'minlovchi axborotni uzatish vositasi emas. Konfidensial ma'lumotlarni uzatishga faqat E-xat xavfsiz elektron pochta tizimi orqali ruxsat beriladi;

har qanday elektron pochta xati, hatto adresatga ma'lum bo'lgan jo'natuvchidan ham, xavf tug'dirishi mumkin, shu nuqtai nazardan, qabul qiluvchi har qanday shubhali elektron pochtadan qo'shimchalarni ochishda juda ehtiyot bo'lishi kerak, hatto u yuboruvchini shaxsan bilsa ham.

41. Foydalanuvchining pochta qutisining o'lchami va uzatiladigan ma'lumotlarning miqdori cheklangan. Agar saqlangan yoki uzatilgan ma'lumotlar hajmi belgilangan chegaradan oshsa, pochtaga kirish bloklanadi. Pochtaga kirish bloklanganda, uning pochta qutisi hajmi chegarasidan oshib ketganligi haqida xabar beriladi va foydalanuvchining pochta qutisini tozalash kerak.

42. Korporativ va Banklararo elektron pochtadan foydalanuvchilarga quyidagilar taqiqlanadi:

shaxsiy yozishmalar uchun, har qanday shaxsiy va tijorat maqsadlarida elektron pochtadan foydalanish;

shifrlanmagan konfidensial ma'lumotlarni yuborish va uzatish;

elektron pochta orqali siyosiy, diniy, g‘ayriinsoniy xarakterdagi ma’lumotlarni, shuningdek, odobsiz, tuhmat, haqoratomuz, tahdid soluvchi yoki noqonuniy materiallarni jo‘natish, namoyish etish va saqlash. Bunday turdagi ma'lumotlar paydo bo'lgan taqdirda, foydalanuvchi darhol o'zining bevosita rahbariga xabar berishi kerak;

axloqsiz mazmundagi, haqoratomuz yoki noqonuniy xarakterdagi, shuningdek tahdid va haqoratlarni o'z ichiga olgan yozishmalarni yuborish;

reklama (asosiy bo'lmagan) va ko'ngilochar materiallarni tarqatish;

ko‘ngilochar telekonferensiyalarga obuna bo‘lish uchun korporativ elektron pochta manzilidan foydalanish, internet tarmog‘idan kasbiy faoliyat yoki xizmat vazifalarini bajarish bilan bog‘liq bo‘lmagan reklama materiallarini davriy ravishda tarqatish;

elektron pochta xabarlarini yuborishda mavjud bo'lmagan qaytarish manzillaridan foydalanish;

unumsiz xatlarni ommaviy jo‘natishni amalga oshirish;

viruslar bilan zararlangan zararli dasturlar yoki fayllarni yuborish;

zararli dasturlar yoki viruslar bilan zararlangan fayllarni, shuningdek *.exe, *.com, *.scr, *.js, *.vbs, *.dll, *.bat va boshqalar kengaytmali bajariladigan fayllarni yuborish;

rasmiy yozishmalar uchun bepul Internet pochta xizmatlaridan (mail.ru, yandex.ru va boshqalar) foydalanish;

har kimga pochta qutingizga kirish uchun parolni taqdim etish;

bankning istalgan axborot tizimlari va resurslariga parollarni elektron pochta orqali yuborish.

43. O'tkazilgan elektron pochta xabari va boshqa elektron hujjatlarning mazmuni qisqa, ixcham va aniq bo'lishi kerak.

44. Quyidagilar qat'iyan man etiladi:

yozishmalar va rasmiy hamda konfidensial axborot almashish uchun ruxsatsiz tashqi pochta xizmatlaridan foydalanish;

korporativ va Banklararo elektron pochta orqali konfidensial ma'lumotlarni uzatish.

VI. Javobgarlik

45. Bank xodimlari ushbu yo‘riqnoma ni buzganlik uchun shaxsan javobgardirlar.

46. Ushbu yo‘riqnoma da belgilangan Internet, elektron pochtadan foydalanish qoidalarini buzish O‘zbekiston Respublikasining ichki mehnat qoidalari va mehnat qonunchiligiga muvofiq intizomiy javobgarlikka sabab bo‘ladi.

47. Xavfsizlik va axborotlarni muhofaza qilish departamenti ushbu yo‘riqnoma ning bank xodimlari tomonidan bajarilishi ustidan nazoratni ta’minlash uchun mas’uldir.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
13-ilova

Axborot aktivlarini boshqarish tartibi

I. Umumiy qoidalar

1. Ushbu hujjat “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – bank)ning axborot aktivlarini aniqlash va ularni himoya qilish uchun tegishli javobgarlikni belgilash maqsadida ularni boshqarish tartibini belgilaydi.

2. Bankning axborot aktivlarini boshqarish tartiblariga quyidagilar kiradi:

a) axborot resurslari va ular bilan bog'liq axborotni qayta ishlash vositalarini aniqlash uchun axborot aktivlarini inventarizatsiya qilish;

b) axborot aktivlarini hisobga olish – ushbu aktivlarning inventarizatsiyasini, shuningdek bank axborot resurslari reyestrini tuzish, uni dolzarbligini ta’minlash;

c) axborot aktivlariga egalik qilish - axborot aktivlari egalarini tayinlash, ularning axborot aktivlariga nisbatan burch va majburiyatlarini belgilash;

d) axborot aktivlarini tasniflash – qonun hujjatlari talablariga muvofiq tasniflash, shuningdek ularni himoya qilishning tegishli darajasini ta’minlash maqsadida bank uchun ahamiyati, muhimligi va sezgirligi;

e) axborot aktivlarini markalash – bank tomonidan qabul qilingan tasniflash tizimiga muvofiq axborot aktivlarini markalash tartib-qoidalari majmuasini ishlab chiqish va amalga oshirish;

f) axborot aktivlaridan maqbul foydalanish va boshqarish - axborot aktivlari va tegishli axborotni qayta ishlash vositalaridan maqbul foydalanish va boshqarish qoidalarini hujjatlashtirish va amalga oshirish.

3. Ushbu tartib bankka tegishli bo‘lgan va bank xodimlari foydalanayotgan axborot aktivlariga nisbatan qo‘llaniladi.

4. Xavfsizlik va axborotlarni muhofaza qilish departamenti bank axborot resurslari reyestrini (keyingi o‘rinlarda - reyestr deyiladi.) ushbu ilovaga muvofiq shaklda shakllantirish va dolzarbligini ta’minlash uchun mas’uldir.

Ushbu tartib ilovasida keltirilgan reyestrga yangi axborot resurslari paydo bo‘lishi munosabati bilan o‘zgartirish va qo‘shimchalar kiritilishi mumkin.

5. Quyidagi axborot aktivlari bank reyestrda hisobga olinishi va boshqarish lozim:

a) qonun talablariga muvofiq himoya qilinishi kerak bo'lgan ma'lumotlarni, shu jumladan tijorat, bank sirlarini va boshqa konfidensial ma'lumotlarni o'z ichiga olgan;

b) bank uchun qadri, ahamiyatli muhim bo‘lgan;

c) avariya va favqulodda vaziyatlarda tiklanish sharti bilan.

Bank axborot aktivlari reyestri elektron shaklda saqlanadigan va qayta ishlanadigan axborot aktivlarini o‘z ichiga oladi.

6. Reyestrga kiritilgan axborot aktivlari Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan belgilanadi.

7. Axborot resurslarining tasnifi bank tomonidan qabul qilingan tasniflash tizimiga muvofiq, reyestrda belgilanishi kerak.

II. Axborot aktivlariga egalik qilish va javobgarlik

8. Axborot resursi (aktivi) egalari hamda Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi quyidagilarga mas'uldirlar:

axborot aktivining mavjudligi, konfidensialligi va yaxlitligini ta'minlash;

axborot aktivining tegishli tasniflanishini ta'minlash;

bank xodimlarining vakolatlarini chegaralash va axborot aktiviga kirishni boshqarish.

9. Axborot resursi (aktivi) egasi axborot aktiviga kirish huquqlarini ta'minlash va ushbu kirishni nazorat qilish uchun javobgardir.

10. Har bir axborot resursi (aktivi) uchun uning qiymatidan kelib chiqqan holda himoya darajasi belgilanadi. Axborot aktivining himoyalanish darajasi Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan axborot aktivi egasi bilan kelishilgan holda belgilanadi.

11. Reyestrni shakllantirish va dolzarbligini ta'minlash, shuningdek, axborot resurslari toifasiga qarab, ularning konfidensialligi, yaxlitligi va mavjudligini ta'minlash bo'yicha talablarni belgilash uchun javobgarlik Xavfsizlik va axborotlarni muhofaza qilish departamenti zimmasiga yuklanadi.

12. Axborot resurslarining axborot xavfsizligini ta'minlash uchun javobgarlik ushbu resurslar egalari zimmasiga yuklanadi va axborot xavfsizligini lozim darajada ta'minlash ustidan nazorat Xavfsizlik va axborotlarni muhofaza qilish departamenti zimmasiga yuklanadi.

III. Axborot aktivlaridan foydalanish

13. Bank axborot aktivlarining egalari bankning aktivning hayotiy sikli (yaratish, saqlash, texnik xizmat ko'rsatish, foydalanish imkoniyatini ta'minlash, axborotni yangilash, xavfsizligini ta'minlash va boshqalar) uchun mas'ul bo'lgan bankning tarkibiy bo'linmalari hisoblanadi.

14. Axborot resurslari (aktivlari) egalari bank tarkibiy bo'linmalari) aniqlanishi va reyestrda ko'rsatilishi shart.

15. Bank axborot aktivi egasiga aktivning barcha ma'lumotlari, axborotni qayta ishlash jarayonlari va tegishli axborotni qayta ishlash vositalari va ilovalari biriktiriladi.

16. Axborot aktiviga egalik qilish huquqi egasi tomonidan boshqa tarkibiy bo'linmaga berilishi mumkin emas. Mazkur bo'linma bank rahbariyatining qaroriga asosan amalga oshiriladi.

17. Axborot aktivining egasi aktivning boshqarilishini ta'minlashi kerak.

18. Axborot aktivlarini boshqarish tartiblari quyidagilardan iborat:

a) axborot aktiviga kirishni ta'minlash va boshqarish;

b) axborot aktivining mavjudligini ta'minlash uchun texnik xizmat ko'rsatish;

c) axborotni yangilash yoki qayta ishlash;

d) axborot aktivi ma'lumotlarining saqlanishi va yaxlitligini ta'minlash;

e) axborot aktivini saqlash;

f) nusxalarini yaratish (replikatsiya) yoki zaxira nusxasini yaratish;

g) nusxa tashuvchilarni markalash;

h) axborot aktivini qaytarish, olib tashlash yoki yo'q qilish va boshqalar.

19. Bank axborot aktivlarining texnik vositalariga texnik xizmat ko‘rsatish Axborot texnologiyalari departamenti xodimlari tomonidan amalga oshiriladi. Axborot aktivlarining egalari bo‘lgan boshqa tarkibiy bo‘linmalarning xodimlari tomonidan axborot aktivlarining texnik vositalariga xizmat ko‘rsatishga faqat bank rahbariyatining qarori bilan amalga oshiriladi.

IV. Axborot aktivlaridan ruxsat etilgan foydalanish

20. Axborot aktividan ruxsat etilgan foydalanish qoidalari axborotga kirish, olish yoki uzatish, foydalanuvchining axborot aktividan foydalanishga qo'yiladigan talablarni belgilashi kerak.

21. Axborot aktividan maqbul foydalanish qoidalari axborot aktivining egasi tomonidan ishlab chiqiladi.

22. Axborot aktivlariga kirish bankning bunday foydalanish huquqiga ega bo‘lgan xodimlari tomonidan olinadi. Bankning ayrim axborot aktivlariga kirish huquqini axborot aktivini yaratish va unga berish maqsadlarini hisobga olgan holda bank mijozlari yoki uchinchi shaxslardan foydalanuvchilar olishlari mumkin.

23. Axborot aktivlaridan foydalanish, shuningdek, axborot aktivini shakllantirish (axborot ta'minoti) bank xodimlari uchun taqdim etiladi. Foydalanuvchilarga foydalanish ruxsati Axborot xavfsizligi siyosatining 10-ilovasida keltirilgan matritsani ishlab chiqish qoidalariga muvofiq shakllantirilgan matritsasiga muvofiq tashkil etiladi.

24. Bank xodimlari axborot aktivlaridan (resurslaridan) o‘z maqsadi bo‘yicha va Axborot aktividan ruxsat etilgan foydalanish qoidalariga muvofiq foydalanishlari shart.

25. Axborot aktivlaridan (resurslaridan) foydalanuvchilar reyestrda ko'rsatilishi shart.

26. Axborot aktivlariga kirish va ulardan foydalanish qoidalari ularning konfidensialligi, yaxlitligi va mavjudligi darajasidan kelib chiqqan holda belgilanishi va Axborot aktivlaridan maqbul foydalanish qoidalarida belgilanishi kerak.

27. "Xizmat maqsadlarida foydalanish uchun", "tijorat siri", "bank siri" yoki "shaxsiy ma'lumotlar" toifasidagi axborot aktivlariga kirish rahbariyat tomonidan tasdiqlangan konfidensial ma'lumotlarga ruxsat berilgan shaxslar ro'yxatiga kiritilgan bank xodimlari tomonidan olinadi. Bank rahbariyati ruxsati Axborot xavfsizligi siyosatining 10-ilovasidagi matritsasiga muvofiq shakllantiriladi.

28. Konfidensial ma'lumotlar toifasiga ega axborot aktivini uchinchi shaxslarga tarqatish taqiqlanadi.

V. Axborot va axborot resurslarining tasnifi

29. Bank axborot-aktivlari (resurslari) ularni himoya qilish talablarini belgilash maqsadida tasniflanadi. Axborot va axborot aktivlarini tasniflash axborot xavfsizligini ta'minlash bo'yicha ishlarni tashkil etishning zarur elementi hisoblanadi.

30. Bank axborot va axborot hujjatlarini tasniflashda quyidagilar e’tiborga olinishi kerak:

axborot tizimining resurslarini (axborot, vazifalar, ish joylari, serverlar, kompyuterlar) ularning mavjudligi, yaxlitligi yoki kirish toifalari buzilgan taqdirda ularni xavf-xatar bo'yicha tasniflash asosida himoya qilishga tabaqalashtirilgan yondashuvning me'yoriy-metodik asoslari;

qonuniy talablar;

bank uchun axborot aktivining qiymati va ahamiyati.

31. Aktivlarni tasniflash, uni davriy ko‘rib chiqish, shuningdek, uning dolzarbligini ta’minlash axborot aktivi egalari hamda Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan amalga oshiriladi.

32. Bank axborot aktivlarini himoya qilishning belgilangan darajasi ularning konfidensialligini, yaxlitligini, mavjudligini va axborotni himoya qilish bo'yicha boshqa talablarning bajarilishini ta'minlashi kerak.

Bankda saqlanadigan va qayta ishlanadigan har xil turdagi ma’lumotlarning turli darajadagi himoyasini ta’minlash zaruratidan kelib chiqib, shuningdek Bankka boshqa tashkilotlarga yoki bank mijozlariga zarar yetkazishning mumkin bo‘lgan usullarini hisobga olgan holda, kirish toifalari , himoyalangan axborot aktivlarining yaxlitligi va mavjudligi joriy etiladi.

33. Axborot va axborot aktivlarining belgilangan sinfiga muvofiq axborot aktiviga kirish va himoyalanishning tegishli darajasi tashkil etilishi kerak.

VI. Axborot va axborot resurslarini tasniflashning asosiy tamoyillari

34. Bank axborot resurslari kirish toifalari bo‘yicha quyidagilarga bo‘linadi:

1) ommaviy axborot resurslari (O) - cheklanmagan foydalanuvchilar doirasi uchun mo'ljallangan;

2) tarqatilishi cheklangan axborot resurslari (XDFU mo'ljallangan;

3) tijorat sirini tashkil etuvchi axborot resurslari (KT);

4) bank sirini tashkil etuvchi axborot resurslari (BT);

5) shaxsiy ma'lumotlarni o'z ichiga olgan axborot resurslari (PD).

35. Konfidensial ma'lumotlarga 2-ilovaga muvofiq konfidensial ma'lumotlar sifatida tasniflangan ma'lumotlar ro'yxatida ko'zda tutilgan, cheklangan tarqatiladigan konfidensial bo'lmagan ma'lumotlar kiradi.

36. Bank axborot resurslari foydalanishning quyidagi toifalariga bo‘lingan:

1) “to’siqsiz foydalana olishlik” (B) - axborot resursiga kirish istalgan vaqtda ta'minlanishi kerak (kechikish bir necha soniya yoki daqiqadan oshmasligi kerak);

2) “yuqori foydalana olishlik” (V) - axborot resursiga kirish sezilarli kechikishlarsiz amalga oshirilishi kerak (kechikish bir necha soatdan oshmasligi kerak);

3) “o’rtacha foydalana olishlik” (C) - axborot resursiga kirish sezilarli vaqt kechikishlari bilan ta'minlanishi mumkin (kechikish bir necha kundan oshmasligi kerak);

4) “quyi foydalana olishlik” (H) - axborot resursiga kirishda kechikishlar deyarli cheksizdir (natijani olishda ruxsat etilgan kechikish bir necha hafta).

37. Bank axborot resurslari himoyalangan axborotning yaxlitligi bo‘yicha quyidagi toifalarga bo‘linadi:

1) “yuqori” (B) - ruxsatsiz o'zgartirish yoki soxtalashtirish jiddiy to'g'ridan-to'g'ri zararga olib kelishi mumkin bo'lgan, yaxlitligi kafolatlangan usullar (masalan, elektron raqamli imzo vositalari) bilan ta'minlanishi kerak bo'lgan axborot resursi. Qonun;

2) “past” (H) - ruxsatsiz o'zgartirish yoki qalbakilashtirish kichik bilvosita zarar etkazishi mumkin bo'lgan axborot resursi, uning yaxlitligi nazorat summalari, xesh-funksiyalar va boshqalarni hisoblash usullari bilan ta'minlanishi kerak;

3) “hech qanday talab yo’q (-) - yaxlitligi talab qilinmaydigan axborot resursi.

VII. Himoyalangan axborotni inventarizatsiya qilish tartibi

38. Bank Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoyalash boshqarmasi aktivlarini aniqlash, reyestrini yuritish va ularni tasniflash maqsadida bank va uning tarkibiy bo‘linmalarida mavjud bo‘lgan axborot resurslarini har yili inventarizatsiyadan o‘tkazadi.

39. Inventarizatsiya jarayonida Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi xodimlari tomonidan bank tarkibiy bo‘linmalari bo‘yicha tur va/yoki so‘rovnoma (anketa to’ldirish) o‘tkaziladi.

40. Axborot aktivlarini inventarizatsiya qilishda quyidagilar aniqlanadi:

yangi va mavjud axborot aktivlarining mavjudligi;

ushbu tartibga muvofiq axborot aktivlarini to‘g‘ri tasniflash va markalash;

foydalanuvchilar ro'yxati va ularning axborot aktividan foydalanish qoidalariga rioya qilishlari;

qayta ishlash talablari va axborot aktividan ruxsat etilgan foydalanish qoidalari va ularni amalga oshirish;

axborot aktivlarini himoya qilish talablarini ular uchun belgilangan xavfsizlik darajasiga muvofiq bajarish;

axborot aktivlari egalari tomonidan ilgari aniqlangan kamchiliklarni bartaraf etish bo'yicha ilgari berilgan ko'rsatmalarning bajarilishi.

41. Inventarizatsiya jarayonida Xavfsizlik va axborotlarni muhofaza qilish departamentining axborotni himoyalash boshqarmasi tomonidan tarkibiy bo‘linmalarda mavjud bo‘lgan axborot resurslari inventarizatsiyasi tuziladi. Har bir axborot resursi uchun ushbu inventar 40-bandga muvofiq ma'lumotlarni o'z ichiga oladi.

42. Inventarizatsiya natijalari axborot resurslarini inventarizatsiya qilish bilan birgalikda Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga ko‘rib chiqish uchun taqdim etiladi.

43. Inventarizatsiya natijalariga ko'ra quyidagi tavsiyalar bilan retseptlar tuziladi:

axborot aktivlari reyestriga va konfidensial ma'lumotlar ro'yxatiga, shu jumladan, axborot aktivlarini tasniflash nuqtai nazaridan o'zgartirish va qo'shimchalar kiritish zarurati to'g'risida;

axborot aktivlarini markalash, qayta ishlash va ulardan foydalanishda aniqlangan kamchiliklarni bartaraf etish;

axborot aktivlari xavfsizligi darajasini oshirish.

Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori tomonidan imzolangan ko'rsatilgan ko'rsatmalar bankning tarkibiy bo'linmalariga beriladi.

44. Inventarizatsiya natijalari bo‘yicha Reyestrga shuningdek, bankning konfidensial ma’lumotlari ro‘yxatiga o‘zgartirish va qo‘shimchalar kiritish bo‘yicha ham takliflar tayyorlanishi mumkin.

VIII. Aktivlarni markirovkalash

45. Bank axborot resurslariga tomonidan qabul qilingan tasniflash bank tizimiga muvofiq, axborotni qayta ishlash jarayonida ularni markalash tartibi qo‘llaniladi.

46. Belgilashning odatiy shakli jismoniy teglash va meta m'lumotlardir (метаданные). Jismoniy yorliq axborot aktivining moddiy tashuvchisiga va/yoki u bilan bog'liq axborotni qayta ishlash vositalariga nisbatan qo'llanilishi mumkin.

47. Axborot aktivlarini markalash ularning egalari tomonidan amalga oshiriladi.

48. Belgilash yorlig'i axborot aktivining seriya raqamini (inventar raqamini), axborot aktivi (tarkibiy birligi) egasini identifikatsiya qiluvchi raqamni, axborot aktivining xavfsizlik sinfini belgilaydigan raqamni ko'rsatadi.

49. Agar markalashdan foydalanish maqsadga muvofiq bo'lmasa, axborot aktivining xavfsizlik sinfini belgilash va ko'rsatishning boshqa vositalaridan foydalanish mumkin.

50. Axborot aktivini tasniflashning har bir darajasi uchun uning egasi qayta ishlash tartibi va axborot aktividan maqbul foydalanish qoidalarini belgilaydi.

Qayta ishlash tartibi va axborot aktividan foydalanish qoidalari quyidagilarni o'z ichiga olishi kerak:

axborot aktivini xavfsiz qayta ishlash, saqlash, uzatish va yo'q qilishga qo'yiladigan talablar;

axborot aktivini qayta ishlashga ruxsat berilgan xodimlar ro'yxati;

axborot aktiviga kiruvchi foydalanuvchilar ro‘yxati;

foydalanuvchilarning axborot aktiviga kirishdagi huquq va majburiyatlari, shu jumladan konfidensial ma'lumotlarni oshkor qilmaslik talablari.

Ushbu tartib axborot aktividan foydalanuvchi tomonidan bajarilishi kerak.

51. Axborot aktivini qayta ishlash va undan foydalanish axborot almashishni nazarda tutuvchi boshqa tashkilotlar bilan tuzilgan shartnomalarga ham kiritilishi kerak. Ma'lumotlarni tasniflash bilan xavfsiz ishlash ma'lumot almashish shartnomalari uchun asosiy talab hisoblanadi.

Axborot aktivlarini boshqarish
Tartibiga ilova

“O‘zsanoatqurilishbank” ATB axborot resurslari reyestri

№	Resurs nomi	Resurs turi	Joylashuvi	Formati	Konf-lik darajasi[1]	Yaxlitligi[2]	Foydalana olishlilik[3]	Ma’ lumotlar yangilanishi davriyligi	Resurs foydalanuvchilari[4]	Resurs egasi[5]
1.	ABT ma'lumotlar bazasi (zaxira nusxalari va elektron arxiv)	Bank mijozlarining bank to‘lovlarini amalga oshirish uchun avtomatlashtirilgan bank texnologiyalari tizimi	ABT ma'lumotlar bazasi serverlari (asosiy va zaxira ma'lumotlarni qayta ishlash markazlari)	Raqamli *.dba	BT, KT, PD	V	B	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti
2.	CRM tizimi ma'lumotlar bazasi	Bank mijozlar bilan munosabatlarni boshqarish tizimi	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli *.dbf	BT, KT, PD	V	B	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti
3.	DWH tizimi ma'lumotlar bazasi	Analitik yoki hisobot ma'lumotlarini yaratish uchun korporativ ma'lumotlar ombori	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli mssql	KT	V	V	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti
4.	CROBS ma'lumotlar bazasi	Biznes jarayonlari va bank vazifalarini avtomatlashtirish tizimi	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli *.dba	KT	V	B	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti

5.	ELMA BPM tizimi ma'lumotlar bazasi	Bankning mijozlarga xizmat ko'rsatish jarayonlarini boshqarish tizimi - kredit konveyeri funksiyasi bilan jismoniy shaxslar	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli Mssql	BT, KT, PD	V	B	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti
6.	EHAT tizimining ma'lumotlar bazasi	Bank ichidagi elektron hujjat aylanishi tizimi	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli Mysql	KT	V	S	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti
7.	SAP tizimi ma'lumotlar bazasi	Byudjetni rejalashtirish tizimi, TSO va POP	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli	KT	V	V	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti
8.	SWIFT tizimi ma'lumotlar bazasi	Bankning xalqaro SWIFT tizimiga ulash tizimi	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli *.dbf	BT, KT	V	B	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti
9.	Ma'lumotlar bazasini qayta ishlash tizimi Way4	Xalqaro plastik kartalarni qayta ishlash tizimi	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli *.dbf	BT, KT, PD	V	B	Uzluksiz ma'lumotlar oqimi	Bank xodimlari	Axborot texnologiyalari departamenti
10.	Internet-Banking tizimining ma'lumotlar bazasi	Internet orqali mijozlarga interaktiv bank xizmatlarini ko'rsatish	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi) (ABT ichida)	Raqamli *.dba	BT, KT, PD	V	B	Uzluksiz ma'lumotlar oqimi	Internet-bank mijozlari	Axborot texnologiyalari departamenti
11.	JOYDA mobil bank ma'lumotlar bazasi	Mobil ilova orqali mijozlarga interaktiv bank xizmatlarini ko'rsatish	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli PostgreSQL	BT, KT, PD	V	B	Uzluksiz ma'lumotlar oqimi	Mobil bank mijozlari	Axborot texnologiyalari departamenti

12.	UzPSB Mobile mobil Banking tizimining ma'lumotlar bazasi	Mobil ilova orqali mijozlarga interaktiv bank xizmatlarini ko'rsatish	Tizim ma'lumotlar bazasi serverlari (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli *.dba	BT, KT, PD	V	B	Uzluksiz ma'lumotlar oqimi	Mobil bank mijozlari	Axborot texnologiyalari departamenti
13.	Bosh ofis va AB fayl serveri	Bankning Bosh ofisi va AB xodimlari uchun fayllarni saqlash	Fayl serverining fayl papkalari (zaxira ma'lumotlarni qayta ishlash markazi)	Raqamli *.doc *.xls *.pdf va boshqalar	KT	H	S	Zarur bo'lganda ma'lumotlarni kiritish	Bankning Bosh ofisi va AB xodimlari	Axborot texnologiyalari departamenti
14.	MBXO va BXM fayl serverlari	MBXO va BXM xodimlarining fayllarini saqlash	Fayl serverining fayl papkalari (zaxira ma'lumotlarni qayta ishlash markazi)	Raqamli *.doc *.xls *.pdf va boshqalar	KT	H	S	Zarur bo'lganda ma'lumotlarni kiritish	MBXO va BXM xodimlari	MBXOning Axborot texnologiyalari bo'limlari
15.	Ichki web-sayt Intranet	Bankning korporativ web sayti	Veb-resurs ma'lumotlar bazasi (asosiy ma'lumotlarni qayta ishlash markazi)	Raqamli *.php	O	H	V	Agar kerak bo'lsa, saytdagi ma'lumotlarni yangilash	Bank xodimlari	Axborot texnologiyalari departamenti
16.	Rasmiy web-sayt	Bank rasmiy sayti	Veb-resurs ma'lumotlar bazasi Unitel ma'lumotlarni qayta ishlash markazi MChJ)	Raqamli *.php Mysql 1C-Bitriks	O	H	V	Agar kerak bo'lsa, saytdagi ma'lumotlarni yangilash	Bank xodimlari, Internet foydalanuvchilari	marketing departamenti, Axborot texnologiyalari departamenti

[1] Konfidensiallik darajasi: XDFU – kirishni cheklanganligi, KT– Tijorat siri, BT – Bank siri, PD – shaxsga doir ma'lumotlar va O - ochiq;

[2] Yaxlitlik: V - yuqori, H – past va «-» (talab mavjud emas);

[3] Foydalana olishlilik: B - to'siqsiz, V - yuqori, S – o'rta, H - past;

[4] Foydalanuvchilar: Bankning bo'linmasiga kirish matritsasi asosida resurs bilan ishlashga ruxsat berilgan;

[5] Egasi: Axborot resursini shakllantirish, ishlatish va xizmat ko'rsatish uchun mas'ul bo'lgan bo'linma.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
14-ilova

Axborotni texnik himoya qilishni tashkil qilish bo’yicha yo’riqnoma

I. Umumiy qoidalar

1. Ushbu yo‘riqnomada axborotni texnik himoya qilishning asosiy chora-tadbirlari, usullari va vositalari, “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda - Bank) ma’lumotlarini himoya qilish tizimiga kiritilgan foydalanuvchilar va mansabdor shaxslarning majburiyatlarini belgilaydi.

2. Ushbu yo‘riqnomaning talablari bank xodimlari uchun majburiydir.

3. Axborotning texnik muhofazasini ta’minlash Xavfsizlik va axborotlarni muhofaza qilish departamenti hamda bank xizmatlari markazlari (keyingi o‘rinlarda MBXO deb yuritiladi) Xavfsizlik va axborotlarni muhofaza qilish bo‘linmalari zimmasiga yuklangan.

4. Xavfsizlik va axborotlarni muhofaza qilish departamenti bankda axborotni texnik muhofaza qilishni tashkil etish bo‘yicha belgilangan talablarning bajarilishini ta’minlaydi va belgilangan talablarning bajarilishini nazorat qiladi.

II. Asosiy tushunchalar va qisqartmalar

5. Ushbu yo‘riqnomada quyidagi atama va ta’rif qo‘llaniladi:

1) **axborotni texnik himoya qilish -** muhandislik va kriptografik bo’lmagan usullardan foydalangan holda axborot xavfsizligini ta’minlashga qaratilgan faoliyat;

2) **axborotni texnik himoya qilish vositalari** - axborotning hayotiy siklining barcha bosqichlarida (axborotni yaratish, uzatish, qabul qilish, o‘zgartirish, namoyish qilish va saqlash) xavfsizlikni ta’minlaydigan apparat, yoki dasturiy ta’minot.

III. Axborotni texnik himoya qilishni tashkil etish tartibi

6. Bankda axborotni texnik himoya qilishni tashkil etish Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan amalga oshiriladi. Quyidagi maqsadlarda mazkur tarkibiy bo'linmalar bilan:

Bankda axborotning texnik himoyasini ta’minlash va axborotni himoya qilish tizimini tashkil etish bo‘yicha talablar ishlab chiqiladi;

xarid qilinadigan axborotni texnik himoya qilish vositalariga qo'yiladigan talablar belgilanadi;

axborot xavfsizligi tizimini rivojlantirish va axborotni himoya qilishning texnik vositalarini joriy etish bo‘yicha rejalar tayyorlanadi;

axborotni himoya qilish tizimini rivojlantirish rejalari doirasida axborotni himoya qilishning texnik vositalarini xarid qilish tashkil etiladi;

ma'lumotlarni texnik himoya qilish tizimi va vositalarini joriy etish va ta'minlashga tayyorgarlik ko'rish bo'yicha tashkiliy chora-tadbirlar ko'rilmoqda, ular

binolarni ajratish, foydalanish yo'riqnomalarini ishlab chiqish, mas'ul xodimni tayinlash va uni ekspluatatsiyaga o'rgatish;

axborotni texnik himoya qilish vositalarini joriy qilishda eksperimental va ekspluatatsiya va qabul qilish sinovlari o'tkaziladi;

axborot xavfsizligi tizimi va uning texnik xavfsizligi vositalaridan foydalanish, jumladan, konfiguratsiya va sozlamalarni monitoring qilish, ish faoliyatini tiklash, dasturiy ta'minot yangilanishlarini o'rnatish, operatsion hujjatlarni yangilash, xavfsizlik hodisalarini kuzatish, nazorat qilish tartiblari va natijalarini hujjatlashtirish;

axborot xavfsizligi tizimining ishlashi va xavfsizligini ta'minlashda kamchiliklar aniqlangan taqdirda uni takomillashtirish bo'yicha takliflar tayyorlanadi va kiritiladi.

7. Konfidensial ma'lumotlarning texnik himoyasini tashkil etilishini amaldagi qonunchilik talablariga rioya qilgan holda ta'minlash.

8. Axborot xavfsizligi tizimi quyidagi bosqichlarda yaratiladi (modernizatsiya qilinmoqda):

loyiha oldidan so'rov o'tkazish, himoya tizimini yaratish (modernizatsiya qilish) zaruriyatini asoslashni ishlab chiqish;

axborotlashtirishni himoya qilish tizimini loyihalash (loyihalarni ishlab chiqish) va joriy etish.

himoya vositalarini tajriba-ekspluatatsion va qabul qilish sinovlarini o'tkazgan holda axborot xavfsizligi tizimini ishga tushirish.

Loyiha oldidan o'tkazilgan so'rov natijalariga ko'ra, axborot xavfsizligi tizimini rivojlantirish bo'yicha texnik topshiriqlar ishlab chiqilmoqda.

Himoya tizimini loyihalash va amalga oshirish bosqichida texnik loyihani ishlab chiqish, tashkiliy-texnik chora-tadbirlarni ishlab chiqish, axborotni himoya qilish vositalarini sotib olish va ularni o'rnatish, kerak bo'lganda, axborot xavfsizligini ta'minlash uchun dasturiy vositalarni ishlab chiqish. amalga oshirildi;

Axborot xavfsizligi tizimini ishga tushirish bosqichida sinovdan o'tkazish, axborot xavfsizligini ta'minlash uchun texnologik jarayonlarni ishlab chiqish, qabul qilish sinovlari o'tkaziladi.

9. Ushbu yo'riqnomada ko'rsatilgan axborotni texnik himoya qilish chora-tadbirlari va vositalari Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan Axborot texnologiyalari departamenti bilan birgalikda amalga oshiriladi.

Ularni amalga oshirish uchun axborot xavfsizligini ta'minlash bo'yicha yillik chora-tadbirlar rejalari tuziladi, shu jumladan axborotni himoya qilishning texnik vositalarini sotib olish, o'rnatish, sozlash, sinovdan o'tkazish va ishga tushirish bo'yicha tadbirlar o'tkazish.

IV. Axborotni texnik himoya qilishning asosiy yo'nalishlari va usullari

10. Axborotni himoya qilish bo'yicha texnik chora-tadbirlar quyidagi asosiy yo'nalishlarda amalga oshirilishi kerak:

tarmoq xavfsizligi;

axborotni zararli dasturlardan himoya qilish;

ruxsatsiz kirishdan himoya qilish;

konfidensial ma'lumotlarni texnik kanallar orqali sizib chiqishidan himoya qilish;

konfidensial ma'lumotlarning chiqib ketishidan himoya qilish;

axborot xavfsizligi hodisalarini kuzatish va ularga javob berish;

axborot xavfsizligini nazorat qilish va tahlil qilish;

imtiyozli foydalanuvchilarni nazorat qilish.

11. Texnik himoya bank axborot infratuzilmasi tarkibiga kiruvchi barcha himoya obyektlari, shu jumladan, bank axborot tizimlari va resurslari bilan ta'minlanadi.

12. Bankda axborot xavfsizligi tizimini yaratish va rivojlantirishda axborot xavfsizligini ta'minlashning texnik usullari joriy etilishi kerak.

V. Axborotni texnik himoya qilishda foydalanilgan usullar va vositalar

Tarmoq xavfsizligi

13. Bankda tarmoq xavfsizligini ta'minlovchi axborotni texnik himoyalash vositalari qatoriga tarmoqlararo ekran, proksi-serverlar, IDPS hujumlarini aniqlash va oldini olish vositalari, WAF web-ilovalari uchun tarmoqlararo ekran kiradi.

14. Bank Axborot xavfsizligi siyosatiga 2-ilovada keltirilgan bank Tarmoq infratuzilmasi darajasida axborot xavfsizligini ta'minlash va tarmoqlararo ekran bilan himoyalanish to‘g‘risidagi nizomga muvofiq tarmoqlararo ekran va himoya devorlaridan foydalanish bo‘yicha chora-tadbirlarni nazarda tutishi kerak.

15. Tarmoqqa tajovuz va hujumlardan himoya qilish IDPS vositalaridan, tarmoqqa ruxsatsiz kirishdan - tarmoqlararo ekran, shu jumladan proksi-serverlar va WAF-dan foydalangan holda ta'minlanishi kerak.

16. Tarmoqlararo ekran, proksi-server va IDPS vositalari sifatida bank apparat-dasturiy va dasturiy vositalardan foydalanadi.

17. Bank quyidagi tarmoq xavfsizligi vositalaridan foydalanadi:

1) Bank korporativ tarmog‘ini Internet tarmog‘iga ulash chegarasida o‘rnatilgan yangi avlod NGFW (xavfsizlik shlyuzi) apparat-dasturiy tarmoqlararo ekran. Asosiy (faol) va zaxira (passiv) xavfsizlik shlyuzlari (“sovuq kutish”) ishlatiladi.

Belgilangan xavfsizlik shlyuzi tarmoqlararo ekran va IDPS vositasi sifatida ishlaydi.

Korporativ tarmoq, bank axborot tizimlari serverlari o‘rnatilgan asosiy ma’lumotlarni qayta ishlash markazi va zaxira ma'lumotlarni qayta ishlash markazi, Bosh ofisning lokal tarmog‘i xavfsizlik shlyuzini tarmoqqa ruxsatsiz kirishdan va tashqi Internet tarmog‘idan tarmoq hujumlaridan himoya qilish obyektlari hisoblanadi.

Xavfsizlik shlyuzining joylashuvi asosiy ma’lumotlarni qayta ishlash markazining server xonasi, zaxira xavfsizlik shlyuzi esa zaxira ma'lumotlarni qayta ishlash markazining server xonasidir.

2) Asosiy ma’lumotlarni qayta ishlash markazini korporativ tarmoqqa ulash chegarasida tarmoqlararo ekran funksiyasi va IDPS vositalariga ega yangi avlod apparat va dasturiy ta'minot NGFW (xavfsizlik shlyuzi) o'rnatilgan. Asosiy (faol) va zaxira (passiv) xavfsizlik shlyuzlari (“sovuq kutish”) ishlatiladi. Bundan tashqari, asosiy ma’lumotlarni qayta ishlash markazini “O‘zbektelekom” AK ma’lumotlar uzatish tarmog‘i orqali korporativ tarmoqqa ulashda apparat-dasturiy tarmoqlararo ekran qo‘llaniladi.

Ushbu xavfsizlik shlyuzi va tarmoqqa ruxsatsiz kirishdan qo‘shimcha tarmoqlararo ekran va korporativ tarmoqdan tarmoqqa himoya qilish obyektlari bank axborot tizimlari serverlari o‘rnatilgan asosiy ma’lumotlarni qayta ishlash markazi hisoblanadi.

Asosiy va zaxira xavfsizlik shlyuzlarining joylashuvi, shuningdek, qo'shimcha tarmoqlararo ekran - asosiy ma'lumotlarni qayta ishlash markazining server xonasi.

3) Tarmoqlararo ekran funksiyasiga ega marshrutizatorlar asosiy ma'lumotlarni qayta ishlash markazining ulanish chegarasida va alohida Bosh ofis (AB) va zaxira ma'lumotlarni qayta ishlash markazining Markaziy bankning BTT ga ulanishi chegarasida o'rnatiladi. Asosiy (faol) va zaxira (passiv) marshrutizatorlar ("sovuq kutish") asosiy ma'lumotlarni qayta ishlash markazida va zaxira ma'lumotlarni qayta ishlash markazida qo'llaniladi.

Ushbu marshrutizatorni Markaziy bank BTT tomonidan tarmoqqa ruxsatsiz kirishdan himoya qilish obyektlari bank axborot tizimlari serverlari o'rnatilgan asosiy ma'lumotlarni qayta ishlash markazi va zaxira ma'lumotlarni qayta ishlash markazi, shuningdek, Bosh ofisning (AB) lokal tarmog'i hisoblanadi.

Mashurtizatorlar joylari asosiy ma'lumotlarni qayta ishlash markazining server xonasi va zaxira ma'lumotlarni qayta ishlash markazining server xonasidir.

4) Bank har bir MBXO, BXM, masofaviy kassalarining korporativ tarmoqqa ulanish chegarasida tarmoqlararo ekran funksiyasiga ega marshrutizatorlar o‘rnatiladi.

Ushbu marshrutizatorlarni korporativ tarmoqdan tarmoqqa ruxsatsiz kirishdan himoya qilish obyektlari lokal tarmoqlar va MBXO resurslari, BXM, bankning masofaviy kassalari hisoblanadi.

Mashurtizatorlarning joylashuvi MBXO va BXM server xonalari, shuningdek masofaviy kassa xonalari.

5) Asosiy ma'lumotlarni qayta ishlash markazining DMZ zonalarini (ABT va boshqa to'lov tizimlari, SWIFT va boshqalar) asosiy ma'lumotlarni qayta ishlash markazining lokal tarmog'iga va korporativ tarmoqqa ulash chegarasida apparat va dasturiy tarmoqlararo ekran o'rnatiladi. Way4 ishlov berish tizimining DMZ zonalarini himoya qilish uchun tarmoqlararo ekran funksiyasi va IDPS vositalariga ega yangi avlod NGFW (xavfsizlik shlyuzi) apparat-dasturiy tarmoqlararo ekran ishlatiladi.

Tarmoqqa ruxsatsiz kirishdan tarmoqlararo ekran va xavfsizlik shlyuzining ma'lumotlarini himoya qilish obyektlari u erda joylashgan axborot tizimlari serverlari joylashgan DMZ zonalari hisoblanadi.

Tarmoqlararo ekran va xavfsizlik shlyuzlari uchun joylar asosiy ma'lumotlarni qayta ishlash markazining server xonalari hisoblanadi.

6) Asosiy ma'lumotlarni qayta ishlash markazini Internetga ulash chegarasida WAF web-ilovalarining apparat-dasturiy himoya devori mavjud.

Ushbu WAF tarmoqlararo ekran Internet tarmog‘idan ruxsatsiz tarmoqqa kirishdan himoya qilish obyektlari bank axborot tizimlarining asosiy ma’lumotlarni qayta ishlash markazida o‘rnatilgan web-ilovalari hisoblanadi. WAF tarmoqlararo ekran barcha kiruvchi web-trafiklarni tekshiradi.

WAF tarmoqlararo ekraning joylashuvi asosiy ma'lumotlarni qayta ishlash markazining server xonasidir.

7) Internetga kirishda proksi-serverlar dasturiy ta'minoti. Uchta proksi-server tashkil etilgan: bank xodimlari uchun asosiy ma’lumotlarni qayta ishlash markazida va

zaxira ma'lumotlarni qayta ishlash markazida proksi-server, asosiy ma'lumotlarni qayta ishlash markazida internet tarmog'idan yangilash maqsadida serverlar uchun proksi-server va Bosh ofis va AB boshqaruv xodimlari uchun yordamchi proksi-server.

Bankning internet tarmog'iga markazlashgan holda ulanishi uchun proksi-serverlar bank xodimlari va alohida serverlarning internet resurslariga kirishiga cheklovlar o'rnatadi va "oq ro'yxat" bo'yicha faqat ruxsat etilgan tashqi axborot resurslariga kirishni ta'minlaydi.

18. 17-bandda ko'rsatilgan himoya vositalaridan foydalanish Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi xodimlari tomonidan amalga oshiriladi.

19. Keraksiz tarmoq trafigini filtrlash uchun xavfsizlik shlyuzlari sozlamalari URL filtri, spam filtri, amaliy qatlam filtri va zararli dasturlar uchun trafikni boshqarish funksiyalaridan foydalanadi.

Zararli dasturlardan himoya

20. Bankda virusga qarshi himoya ish stansiyalari va serverlarida o'rnatilgan zararli dasturlardan antivirus himoyasini qo'llash orqali ta'minlanadi.

21. Bank antivirus dasturlarini markazlashgan holda boshqarishning litsenziyalangan tizimidan foydalanadi.

Ushbu antivirus tizimi quyidagilardan iborat:

asosiy ma'lumotlarni qayta ishlash markazida o'rnatilgan markaziy server, undan Bankda antiviruslarni markazlashtirilgan yangilash amalga oshiriladi va ulardan antivirus xavfsizligini buzish holatlari to'g'risida ma'lumotlar yig'iladi;

MBXOdagi ish stansiyalarida o'rnatilgan antiviruslarning ishlashi va boshqaruvini nazorat qilish uchun har bir MBXOda yordamchi serverlar va unga bo'ysunuvchi BXM, masofaviy kassalar, ushbu server MBXO server xonasida joylashgan;

har bir ish stansiyasida o'rnatilgan antiviruslar va Bankda foydalaniladigan serverlar.

Markazlashtirilgan virusga qarshi tizim Bosh ofis, AB, MBXO va ularga bo'ysunuvchi BXM, masofaviy kassalarning ish stansiyalarida o'rnatilgan barcha antiviruslarni boshqarishni ta'minlaydi.

22. Bank ish stansiyalari va serverlari virusga qarshi himoya qilish obyektlari hisoblanadi.

23. Antivirusdan himoya qilish bank Axborot xavfsizligi siyosatiga 8-ilovada keltirilgan virusga qarshi himoya qilish bo'yicha yo'riqnomaga muvofiq tashkil etilishi va ta'minlanishi kerak.

24. Bundan tashqari, bank tarmoq trafigida zararli dasturlarni aniqlash va zararsizlantirish funksiyasiga ega xavfsizlik shlyuzlaridan (tarmoqlararo ekran va IDPS vositalari) foydalanadi.

25. Antivirus himoya vositalarining ishlashi Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi xodimlari va MBXOning Xavfsizlik va axborotni muhofaza qilish bo'limi xodimlari tomonidan amalga oshiriladi.

Ruxsatsiz kirishdan himoyalash

26. Bank ruxsat etilmagan jismoniy kirishdan himoya qilishning quyidagi texnik usullarini nazarda tutadi:

ruxsatsiz jismoniy kirishni oldini oluvchi yoki blokirovka qiluvchi qulflar (mexanik, elektromexanik, elektr), muhrlar bilan jihozlangan muhandislik himoya vositalaridan (eshiklar, devorlar, shiftlar, derazalardagi panjaralar, to'siqlar, to'siqlar va boshqalar) foydalanish;

axborotni qayta ishlash, saqlash va uzatishning tashqi korpusida bir martalik plomba, himoya yopishqoq lenta yoki himoya va gologrаfik yorliqlardan foydalanish;

xavfsizlik signalizatsiyasi va video kuzatuv tizimini o'rnatish;

SKUDdan foydalanish.

27. Axborotni qayta ishlash, saqlash va uzatish vositalariga, yagona domen tarmog'iga, bank axborot resurslari va tizimlariga ruxsatsiz tarmoq kirishidan himoya qilish uchun foydalanuvchi autentifikatsiya vositalaridan foydalaniladi.

28. Bank yagona domen tarmog‘ida tarmoq resurslariga (tarmoq fayllari omborlari, printerlar, ish stansiyalari va boshqalar), axborot tizimlariga kirishni nazorat qilish, chegaralash va boshqarish hamda foydalanuvchi va ish stansiyasi hisoblarini yuritish, xizmat ko‘rsatish kataloglari (Katalog xizmati) bank domen kontrolleri serverlarida.

29. Tarmoq resurslariga kirishni farqlash Active Directory tizim administratori tomonidan sozlangan bank domen kontrolleri serverlarida, shuningdek, tarmoqlararo ekran yordamida ta'minlanadi.

Bank Bosh ofis, AB, BXM, masofaviy kassalar uchun yagona domendan foydalanadi. Shuningdek, Way4 bank plastik kartochkalarini qayta ishlash tizimi va unga ulangan bankning tegishli tarkibiy bo‘linmalari uchun alohida domen kontroller serveri yordamida alohida boshqariladigan domen tarmog‘i yaratiladi.

Bankning domen nazoratchisi serverlari asosida Bosh ofis, MBXO, masofaviy kassalar xodimlari uchun kirishni farqlashni ta'minlaydigan Active Directory guruh siyosatlari yaratilgan. Bank Axborot xavfsizligi siyosatiga 10-ilovaga muvofiq “Kirish matritsasi”ga muvofiq axborot tizimlari va tarmoq qurilmalariga ruxsat etiladi.

Bankning domen kontrolleri serverlarining joylashuvi bank asosiy va zaxira ma’lumotlarni qayta ishlash markazining server xonasi hisoblanadi.

30. Bank axborot tizimlaridan foydalanuvchilarning foydalanishi ularda qo‘llaniladigan nazorat qilish va kirishni nazorat qilish vositalari bilan cheklanadi, ular bank axborot tizimlari administrator tomonidan boshqariladi. (ABT uchun administrator buxgalteriya hisobi va moliyaviy menejment departamenti).

Bankning har bir axborot tizimida tizim foydalanuvchilarining login va paroli asosida dasturiy ta’minotni boshqarish va kirishni nazorat qilish joriy etilgan va foydalanilmoqda.

Bundan tashqari, login va parol bilan bir qatorda ERI foydalanuvchi autentifikatsiyasi uchun ABT da qo'llaniladi.

31. Bankning axborotlashtirish obyektlariga kirishni monitoring qilish, chegaralash va boshqarish tizimi bank axborot xavfsizligi siyosatiga 7-ilovada keltirilgan parolni himoyalash va autentifikatsiya qilish bo‘yicha yo‘riqnoma talablariga muvofiq tashkil etilishi kerak”.

32. Bankka kirishni farqlash bank axborot xavfsizligi siyosatiga 10-ilovada keltirilgan axborot resurslaridan foydalanish Matritsasiga muvofiq amalga oshirilishi kerak.

Texnik kanallar orqali ma'lumotlarning sizib chiqishidan himoya qilish

33. Texnik kanallar orqali ma'lumot sizib chiqishidan himoya qilishning asosiy usullari quyidagilardan iborat:

axborotni uzatish, qayta ishlash va saqlashda sertifikatlangan texnik vositalar va tizimlardan foydalanish;

qo'riqlanadigan obyektni bino perimetridan maksimal mumkin bo'lgan masofada joylashtirish;

qo'riqlanadigan binolar ro'yxati va ulardan foydalanish uchun javobgar shaxslar haqidagi ma'lumotlarni to'liq hujjatlashtirilishi;

himoyalangan xonalarni jihozlash bo'yicha tavsiya etilgan tadbirlarni amalga oshirish: devorlar, pollar va shiftlar boshqa tashkilotlarning binolari yonida bo'lmasligi derazalar esa pardalar bilan yopilgan bo'lishi kerak.

ma'lumotlarning sizib chiqishi texnik kanallari mavjudligini aniqlash uchun binolarda maxsus tekshirishlar o'tkazish;

nutq signalini faol himoya qilish vositalaridan foydalanish (shovqin generatorlari va boshqalar).

34. Texnik kanallar orqali sizib chiqishdan himoya qilish bo'yicha chora-tadbirlarni amalga oshirishni tashkil etish va nazorat qilish Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi va MBXO Xavfsizlik va axborotni muhofaza qilish bo'limlari tomonidan amalga oshiriladi.

Konfidensial ma'lumotlarni chiqib ketishdan himoya qilish

35. Bank axborot tizimidan konfidensial ma'lumotlarni sizib chiqib ketishdan himoya qilish maqsadida konfidensial axborot sizib chiqishining oldini olish (DLP) tizimi qo'llaniladi.

36. DLP tizimi konfidensial ma'lumotlarning sizib chiqishining barcha mumkin bo'lgan kanallarini nazorat qilishi, bank axborot tizimidagi konfidensial ma'lumotlar va ular bo'yicha ko'rilgan choralarning qaydini olib borishi, sizib chiqish holatlarini aniqlash va hisobot berish, qoidabuzarlarni aniqlash, qonunbuzarliklarning rad etib bo'lmaydigan dalillarini to'plash va saqlashi kerak.

37. Bank DLP tizimining dasturiy vositasidan foydalanadi.

DLP tizim serveri bank asosiy ma'lumotlarni qayta ishlash markazining server xonasiga o'rnatilgan.

38. Bankda DLP tizimi Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan boshqariladi.

Axborot xavfsizligi hodisalarini monitoring qilish va ularga javob berish

39. Bankda axborotni avtomatik to'plash va axborot xavfsizligi hodisalari va hodisalarini boshqarish uchun quyidagi monitoring dasturiy vositalari qo'llaniladi:

SIEM axborot xavfsizligi monitoringi va hodisalarni boshqarish tizimlari;

muhim uskunalarning ishlashini monitoring qilish va so'rovlar va bank resurslarining yuklanishini monitoring qilish tizimlari;

tarmoqlararo ekrandan jurnallarni yig'ish va qayta ishlash tizimlari.

40. Bankda qo‘llaniladigan axborot xavfsizligi hodisalarini kuzatish va ularga javob berish vositalariga Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi xizmat ko‘rsatadi.

Axborot xavfsizligini ta’minlanganlik holatini tahlil va nazorat qilish

41. Xavfsizlikni tahlil qilish va nazorat qilishni ta’minlash uchun bank xavfsizlikni tahlil qilish va nazorat qilish dasturiy vositalaridan foydalanadi.

42. Xavfsizlikni tahlil qilish va nazorat qilish maqsadida bank maxsus xavfsizlik skanerlaridan foydalanishni nazarda tutadi.

43. Xavfsizlik tahlili natijalariga ko‘ra, bank axborot xavfsizligi tizimida axborot xavfsizligi darajasini oshirish va aniqlangan zaifliklar va kamchiliklarni bartaraf etish bo‘yicha tegishli choralar ko‘rilsin.

44. Xavfsizlikni nazorat qilish va tahlil qilish Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan amalga oshiriladi.

Imtiyozli foydalanuvchi nazorati

45. Bank axborot tizimlariga xizmat ko‘rsatuvchi administratorlarning xatti-harakatlarini nazorat qilish, ular tomonidan imtiyozli huquqlarni suiiste’mol qilish faktlarini aniqlash shuningdek, ular tomonidan axborot tizimlari ma’lumotlar bazasidan ma’lumotlarning chiqib ketishiga yo‘l qo‘ymaslik uchun bank imtiyozli foydalanuvchilarni kuzatish uchun dasturiy vosita - PAM tizimi.

46. PAM tizimini saqlash va imtiyozli foydalanuvchilarning harakatlarini nazorat qilish Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan amalga oshiriladi.

VI. Axborotni texnik himoya qilish choralari va vositalarini qo’llash

47. Texnik axborotni himoya qilish vositalaridan foydalanish Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi xodimlari va MBXO Xavfsizlik va axborotni muhofaza qilish bo’limi xodimlari tomonidan Axborot xavfsizligi siyosati talablariga muvofiq amalga oshiriladi. Bank, shuningdek, texnik va dasturiy ta’minot axborotni himoya qilish vositalarini ishlatish bo‘yicha yo‘riqnoma va qo‘llanmalarga muvofiq amalga oshiradi.

48. Axborot xavfsizligini ta’minlashning texnik va dasturiy vositalarini ishlatish bo‘yicha yo‘riqnoma va qo‘llanmalar Bankda joriy etilgan va qo‘llaniladigan har bir texnik xavfsizlik vositasiga nisbatan Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan ishlab chiqiladi. Ushbu ko'rsatmalar ushbu vositalarni ishlab chiquvchilar yoki ishlab chiqaruvchilarning qo'llanmalari va operatsion hujjatlari asosida ishlab chiqilgan.

VII. Javobgarlik

49. Xavfsizlik va axborotlarni muhofaza qilish departament ushbu yo‘riqnomaga muvofiq axborotni texnik muhofaza qilish chora-tadbirlarini amalga oshirish uchun javobgardir.

50. Ushbu yo'riqnomada belgilangan talablarni buzish O'zbekiston Respublikasining ichki mehnat qoidalari va mehnat qonunchiligiga muvofiq intizomiy javobgarlikka sabab bo'ladi.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
15-ilova

Axborotni kriptografik himoyalashni tashkil etish bo‘yicha yo’riqnoma

I. Umumiy qoidalar

1. Ushbu yo‘riqnoma “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank) axborot xavfsizligi tizimiga kiritilgan asosiy chora-tadbirlar, axborotni kriptografik himoyalash usullari va vositalarini hamda ularni amalga oshirish tartibini belgilaydi, shuningdek, axborotni kriptografik himoyalash vositalari (keyingi o‘rinlarda AKH deb ataladi) va elektron raqamli imzo kriptografik kalitlari (keyingi o'rinlarda - ERI)bilan ishlashga vakolatli bank xodimlarining harakatlarini tartibga soladi.

2. Ushbu yo‘riqnoma talablari Bankda qo‘llanilishi va uning xodimlari tomonidan bajarilishi majburiydir.

3. Bankda axborotning kriptografik himoyasi quyidagilar uchun qo‘llaniladi:

bank xodimlari tomonidan avtomatlashtirilgan bank tizimida (keyingi o‘rinlarda ABT deb yuritiladi) ma’lumotlar almashishda hamda yuridik shaxs bo‘lgan bank mijozlari tomonidan internet-Banking va mobil Banking xizmatlaridan foydalanishda ma’lumotlarning muallifligi va yaxlitligini ta’minlash maqsadida ERIni shakllantirish va tekshirish;

ABT foydalanuvchilari va Internet-Banking va mobil Banking mijozlarini autentifikatsiya qilish uchun ERIni shakllantirish va tekshirish;

bank xodimlari tomonidan elektron hujjat aylanish tizimida (keyingi o‘rinlarda ERI tizimi deb yuritiladi) axborot almashishda ma’lumotlarning muallifligi va yaxlitligini ta’minlash uchun ERIni shakllantirish va tekshirish;

uzatilayotgan axborotni shifrlash, ERI yaratish va tekshirishni ta’minlovchi E-xat tizimidan foydalangan holda xavfsiz axborot almashinuvi;

Bankda xavfsiz ulanishni tashkil etish.

4. Axborotning kriptografik himoyalashni ta’minlash Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi zimmasiga hisoblanadi.

5. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi bankda axborotni kriptografik himoyalashni tashkil etish bo‘yicha belgilangan talablarning bajarilishini ta’minlaydi va belgilangan talablarning bajarilishini nazorat qiladi.

6. Bankda qo‘llaniladigan AKH O‘zbekiston Respublikasi Prezidentining 2007-yil 3-apreldagi “O‘zbekiston Respublikasida axborotni kriptografik himoyalashni tashkil etish chora-tadbirlari to‘g‘risida”gi PQ-614-son Farmoniga muvofiq sertifikatlangan bo‘lishi kerak.

II. Asosiy tushunchalar va qisqartmalar

7. Ushbu yo‘riqnomada quyidagi atamalar va ta’riflar qo‘llaniladi:

1) **kriptografik algoritm (kriptoalgoritm)** - ma’lumotlarni buzib ko‘rsatish va ruxsatsiz kirishdan himoya qilish maqsadida ma’lumotlarni (axborotni) o‘zgartirishning matematik algoritmi;

2) **axborotni kriptografik himoyalash** - kriptografik o‘zgartirish algoritmlari (kriptoalgoritmlar) yordamida amalga oshiriladigan axborotning yaxlitligini, erkinligini va maxfiyligini ta’minlashga qaratilgan chora-tadbirlar majmui;

3) **axborotni kriptografik himoyalash vositalari (AKH)** - axborotning xavfsizligini ta’minlash uchun axborotning kriptografik o‘zgartirilishini amalga oshiradigan apparat, dasturiy yoki apparat-dasturiy vositalar:

a) **shifrlash vositalari** - Axborotni almashtirish kriptografik algoritmlarini amalga oshiruvchi va axborotni qayta ishlash, saqlash hamda aloqa kanallari bo’ylab uzatishda uni ruxsatsiz foydalana olishdan muhofaza qilish uchun mo’ljallangan apparat, dasturiy yoki apparat-dasturiy vositalar.

b) **elektron raqamli imzo vositalari** - Elektron hujjatda elektron raqamli imzo yaratilishi, elektron raqamli imzo haqiqiyligining tasdiqlanishi, elektron raqamli imzo ochiq va yopiq kalitlarining yaratilishini ta’minlovchi texnik va dasturiy vositalar jami.

4) **kriptografik kalit** - kriptografik algoritmlardan foydalangan holda elektron imzolarni shifrlaydigan, parolini ochadigan, yaratadigan va tekshiradigan maxfiy belgilar ketma-ketligi;

5) **kriptografik tizim (kriptotizim) -** axborotni kriptografik o'zgartirishni va (yoki) boshqarishni, shu jumladan avtomatlashtirilgan, kriptografik kalitlarni ishlab chiqarish va tarqatish jarayonini ta'minlaydigan tashkiliy, texnik va dasturiy vositalar to'plami;

6) **shifrlash:** kriptografik algoritmga va ma’lumotlarning haqiqiy tarkibini ishonchli yashirish uchun kalitga muvofiq ma’lumotlarning (axborotlarning) qayta tiklanadigan o‘zgarishlari to‘plami.

III. Axborotning kriptografik himoyasini tashkil etish tartibi

8. Bankda axborotni kriptografik himoyalashni tashkil etish Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan ta’minlanadi. Shu maqsadda ushbu tarkibiy bo'linma:

Bankda axborotning kriptografik himoyasini ta’minlash va AKH dan foydalanish bo‘yicha talablar ishlab chiqadi;

kriptografik tizimni ishlab chiqish va AKHni amalga oshirish bo'yicha rejalar tayyorlaydi;

AKH uchun talablar ishlab chiqiladi, ularni sotib olish, joriy etish va ishga tushirish va sertifikatlash tashkil etadi;

kriptografik tizim va unga kiritilgan AKHning ishlashi amalga oshiradi.

9. Ushbu yo'riqnomada ko'rsatilgan ma'lumotlarni kriptografik himoya qilish choralari va vositalari Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan MBXO Xavfsizlik va axborotni muhofaza qilish bo'limlari bilan birgalikda amalga oshiriladi.

Ularni amalga oshirish uchun axborot xavfsizligini ta'minlash bo'yicha yillik chora-tadbirlar rejalari, shu jumladan AKHni amalga oshirish va undan foydalanish bo'yicha chora-tadbirlar ishlab chiqiladi.

10. AKHning ishlashi bank xodimlari tomonidan ushbu AKHni ishlab chiquvchilar (ishlab chiqaruvchilar) tomonidan ularning ishlashi bo'yicha ko'rsatmalarga muvofiq amalga oshiriladi.

11. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi va MBXOning Xavfsizlik va axborotni muhofaza qilish bo'limlari xodimlari quyidagilarni amalga oshiradi:

bank xodimlari uchun AKHni o'rnatish va sozlash;

asosiy bank tizimi va ERI tizimi foydalanuvchilari bo‘lgan bank xodimlariga, yuridik shaxs bo‘lgan internet-Banking va mobil Banking mijozlariga xavfsiz USB-tashuvchilarda ERIni tekshirish va yaratish uchun kriptografik kalitlarni hisobga olish, berish va yaratish;

bank xodimlari va Internet-Banking va mobil Banking mijozlari uchun ERI ochiq kalit sertifikatlarini ishlab chiqarish.

bank ERI kalitlarini ro‘yxatdan o‘tkazish markazi faoliyati Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi xodimlari tomonidan amalga oshiriladi.

12. AKH faoliyati bo‘yicha yo‘riqnomalar bank xodimlariga Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan yetkaziladi.

IV. Axborotni kriptografik himoyalash usullari va vositalari

13. Bankda AKH qo‘llaniladi:

1) Bank xodimlari ABT uchun ERIni shakllantirish va tekshirish;

2) Internet-Banking va mobil Banking mijozlari uchun interaktiv bank xizmatlaridan foydalanganda ERIni shakllantirish va tekshirish;

3) E-xat xavfsiz elektron pochta tizimida alohida bank xodimlari tomonidan (ma’lumotlarni shifrlash, ERI shakllantirish va tekshirish) uchinchi shaxslar bilan tizim orqali ma’lumotlarning xavfsiz uzatilishini ta’minlash.

14. ABT va ERI tizimi O'zDSt 1092-2009 standartiga muvofiq ERIni (keyingi o'rinlarda ERI vositasi deb yuritiladi) shakllantirish va tekshirishni ta'minlovchi AKH dasturiy ta'minotidan foydalanadi.

ERI vositasi ABT va EHAT tizimining vakolatli foydalanuvchilari bo'lgan bank xodimlarining ish stansiyalariga o'rnatiladi.

15. ABT tizimiga elektron to‘lov hujjatlarini kirituvchi, tasdiqlovchi va tegishli operatsiyalarni amalga oshiruvchi, shuningdek, ERI tizimining foydalanuvchilari bo‘lgan barcha mas’ul bank xodimlari ABT va EHAT tizimida qo‘llaniladigan ERI kriptografik yopiq kalitlari bilan ta’minlanishi kerak.

16. ERI kriptografik kalitlari kalitlarini ro‘yxatga olish markazi dasturiy ta’minotidan foydalangan holda Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan ABT va EHAT tizimining ruxsat etilgan foydalanuvchilari hisoblangan bank xodimlariga ishlab chiqariladi va beriladi.

Kriptografik ERI kalitlarini yaratish jarayoni himoyalangan bo'lishi kerak.

17. Bank xodimlari (ABT foydalanuvchilari) uchun yaratilgan ERI kriptografik kalitlari xavfsiz USB-tashuvchida qayd etilgan.

18. ERI kriptografik kalitlarini berish, ularni ABT va EHAT tizimidan foydalanuvchi bank xodimlariga rejali va rejadan tashqari o‘zgartirish tartibi bank axborot xavfsizligi siyosatiga 7-ilovada keltirilgan parolni himoya qilish va autentifikatsiya qilish bo‘yicha yo‘riqnomada belgilangan..

19. Bank xodimlarining ERIni tekshirish uchun bank ERI kalitlarini ro‘yxatga olish markazi tomonidan ERI ochiq kalitlari sertifikatlari ishlab chiqariladi, ular Ro‘yxatga olish markazining ma’lumotlar bazasiga kiritiladi.

20. Internet-Banking va mobil Banking tizimlarida O'zDSt 1092-2009 standartiga muvofiq ERIni yaratish va tekshirishni ta'minlash uchun ERI dasturiy vositasi qo'llaniladi. ERI vositasi to'g'ridan-to'g'ri foydalanuvchining ish stansiyasiga yoki mobil qurilmasiga o'rnatiladi.

Internet-Banking va mobil Banking tizimlarida qo‘llaniladigan ERI ochiq kalitlarining shaxsiy kalitlari va sertifikatlari bank ERI kalitlarini ro‘yxatdan o‘tkazish markazi tomonidan ishlab chiqariladi va foydalanuvchilarga ularning Bankka murojaati asosida beriladi.

21. Bank ERI kalitlarini ro‘yxatdan o‘tkazish markazi tomonidan berilgan ERI kaliti sertifikatining amal qilish muddati ERI ro‘yxatdan o‘tkazilgan kundan boshlab 24 oydan oshmasligi kerak.

ERI kriptografik shaxsiy kalitlari ERI ochiq kalit sertifikatining amal qilish muddati tugagandan so'ng o'zgartirilishi kerak.

22. AKH E-xat xavfsiz elektron pochta tizimida ma'lumotlarning tizim orqali xavfsiz uzatilishini ta'minlash uchun ishlatiladi.

Bank xodimlari orasidan E-xat tizimidan foydalanuvchilar bank boshqaruvi tomonidan belgilanadi.

E-xat tizimi foydalanuvchilariga kriptografik shifrlash kalitlari va ERI, shuningdek tizimlardagi ERI asosida foydalanuvchi autentifikatsiyasini, kiritilgan va uzatiladigan ma’lumotlarni shifrlashni, shuningdek, ERIni shakllantirishni ta’minlovchi ERI ochiq kalit sertifikatlari beriladi. uzatish paytida uning yaxlitligini ta'minlash uchun kiritilgan ma'lumotlar.

Kriptografik shifrlash kalitlari va ERI, shuningdek ERI ochiq kalitlari sertifikatlari bank xodimlari bo‘lgan E-xat tizimi foydalanuvchilariga xavfsiz USB-tashuvchida ishlab chiqariladi va beriladi.

Bank E-xat xizmatlarini ko‘rsatish bo‘yicha kriptografik shifrlash kalitlari va ERIlarni yaratish hamda ERI ochiq kalit sertifikatlarini shakllantirish “UNICON.UZ” DUK va o‘rtasida tuzilgan shartnoma asosida belgilangan tartibda ro‘yxatdan o‘tgan “UNICON.UZ” DUK tomonidan ERI kalitlarini ro‘yxatga olish markazi tomonidan amalga oshiriladi. .

E-xat tizimida O'zDSt 1092-2009 standartiga muvofiq ERI (ERI vositasi) ni shakllantirish va tekshirishni ta'minlovchi "UNICON.UZ" DUK AKH dasturiy ta'minoti va mos ravishda uzatilayotgan axborotni (shifrlash vositasi) kriptografik shifrlashdan foydalaniladi. O'zDSt 1105-2009 standarti bilan. AKH xavfsiz USB-tashuvchisiga o'rnatilgan bo'lib, u ERIni shakllantirish va tekshirishni, shuningdek, tizim foydalanuvchisi tomonidan ish stansiyasiga ulanganida shifrlashni ta'minlaydi.

AKH bank xodimlarining ish stansiyalarida va E-xat tizimining mijoz dasturlarini o‘rnatish va sozlash Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi tomonidan amalga

oshiriladi.

23. Bankda xavfsiz ulanishni tashkil qilish uchun ham qo‘llaniladi:

a) foydalanuvchilar AES va 3-DES assimetrik shifrlash kriptografik algoritmlaridan foydalangan holda bankning tashqi web-resurslariga (rasmiy web-sayti, Internet-Banking va boshqalar) ulanishini ta'minlashda https, SSL/TLS protokollaridan foydalangan holda xavfsiz https ulanishlaridan foydalanish va xesh-funksiyalar –SHA-1;

b) AES-CBC assimetrik shifrlash kriptografik algoritmlari, xesh-funksiyalari – SHA-3 va EDS - RSA-dan foydalangan holda mobil Bankingdan foydalanishda bank mijozlarining mobil ilovadan ulanishini ta'minlashda TLS protokolidan foydalangan holda xavfsiz ulanishlardan foydalanish;

c) IPSec protokoli va kriptografik shifrlash algoritmlari - 3-DES va xesh funksiyalari – SHA-1 yordamida xavfsiz VPN ulanishlaridan foydalanish.

Kriptografik kalitlarni yaratish va saqlash web-ilovalar va VPN vositalariga o'rnatilgan AKH tomonidan amalga oshiriladi.

VPN texnologiyalaridan foydalangan holda va IPSec protokolidan foydalangan holda xavfsiz ulanishlarni tashkil qilish uchun Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi mas'uldir.

Https, SSL/TLS protokollaridan foydalangan holda xavfsiz ulanishlarni tashkil qilish uchun Axborot texnologiyalari departamentining Raqamli texnologiyalar va masofaviy bank tizimlarini qo'llab-quvvatlash bo'limi mas'uldir.

24. Bankda qo‘llanilayotgan AKH belgilangan tartibda sertifikatlangan bo‘lishi kerak.

25. Kriptografik kalitlardan faqat ularning egalari foydalanishi kerak.

V. AKHdan foydalanishda xodimlarning majburiyatlari va javobgarliklari

26. Kriptografik ERIkalitlari bilan ishlaydigan bank xodimlari quyidagilarga majburdirlar:

ERI kriptografik kalitlarining xavfsizligini ta'minlash va ulardan foydalanilmagan taqdirda ularni xavfsiz joylarda (seyflarda) saqlash;

ERI kriptografik kalitlarini o‘tkazmaslik, shuningdek, ERI kriptografik kalitiga kirish parollarini bankning boshqa xodimlari va ruxsati bo‘lmagan shaxslarga oshkor qilmaslik;

agar ERI kriptografik kalitlari ishlatilmasa (ish kuni tugashi, ta'tilga yoki kasallik tufayli ta'tiliga chiqish va h.k.), uni o'z tarkibiy bo'linma rahbariyatiga yoki Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi va MBXOning Xavfsizlik va axborotni muhofaza qilish bo’limiga topshiriladi. bank xodimlarining foydalanilmagan kriptografik ERI kalitlari seyflarda saqlanishi kerak;

ishdan bo'shatilganda yoki AKHdan foydalanish bilan bog'liq vazifalarni bajarishdan chetlashtirilganda ERI kriptografik kaliti bilan himoyalangan USB-tashuvchini qaytarish;

taqdim etilgan xavfsiz USB axborot vositalaridan kriptografik kalitlarni saqlashdan boshqa maqsadlarda foydalanmaslik.

27. Xodim yo‘qligida yoki axborot tizimlarida ishlamayotgan vaqtda ERI kriptografik kalitlarining himoyalangan USB-tashuvchini ish joyida qarovsiz qoldirmaslik.

28. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasiga quyidagi hollarda zudlik bilan xabar berish: ERI kriptografik kaliti yo'qolishi va o'g'irlanishi, ERI kriptografik kalitining buzilganligi, ABT tizimiga kirish bilan bog'liq muammolar ERI kriptografik kalitining himoyalangan USB-tashuvchiga zarar yetkazilishi oldini olish.

29. Muvaffaqiyatsiz ERI kriptografik kalitlari va/yoki himoyalangan USB qurilmalar keyinchalik almashtirish uchun Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasiga yoki MBXOning Xavfsizlik va axborotni muhofaza qilish bo’limiga belgilangan tartibda qaytariladi.

30. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi hamda MBXOning Xavfsizlik va axborotni muhofaza qilish bo‘limlari bank xodimlariga va ularning tashuvchilariga berilgan ERI kriptografik kalitlari va ularning tashuvchilari qayd etilishini maxsus jurnallar bilan ta’minlashi shart.

VI. Javobgarlik

31. Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi va MBXOning Xavfsizlik va axborotlarni muhofaza qilish departamenti ushbu yo'riqnomaga muvofiq kriptografik axborotni himoya qilish choralarini amalga oshirish uchun javobgardir.

32. AKH bilan ishlaydigan bank xodimlari ushbu Yo'riqnoma talablarini buzganlik uchun shaxsan javobgardirlar.

33. Bank xodimlari tomonidan ushbu yo‘riqnoma ning bajarilishi ustidan nazoratni ta’minlash uchun Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi hamda MBXOning Xavfsizlik va axborotni muhofaza qilish bo‘limlari mas’uldirlar.

34. Ushbu Yo'riqnomada belgilangan talablarni buzish O'zbekiston Respublikasining ichki mehnat qoidalari va mehnat qonunchiligiga muvofiq intizomiy javobgarlikka sabab bo'ladi.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
16-ilova

Konfidensial ma'lumotlarni himoya qilish to'g'risida yo’riqnoma

I. Umumiy qoidalar

1 . Ushbu yo‘riqnoma “O‘zsanoatqurilishbank” ATB (keyingi o‘rinlarda – Bank)da konfidensial ma'lumotlar himoyasini ta'minlashni tashkil etish tartibi va talablarini O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015 yil 16 oktyabrdagi “O‘zbekiston Respublikasi axborotlashtirish obyektlarida konfidensial axborotni saqlashni tashkil etish va xavfsizligini ta'minlash tartibi to‘g‘risidagi nizomni tasdiqlash to‘g‘risida”gi 295-son qarori hamda O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari – Davlat sirlarini himoya qilish masalalari bo‘yicha idoralararo komissiya Raisi tomonidan 2006-yil 5-dekabrda tasdiqlangan, maxfiy bo‘lmagan, tarqatilishi cheklangan ma'lumotlarni o‘z ichiga olgan hujjatlar, fayllar va nashrlarni hisobga olish, muomalada bo‘lish va saqlash tartibi to‘g‘risidagi yo‘riqnomaga muvofiq tartibini belgilaydi.

2. Ushbu yo‘riqnoma davlat sirlarini o‘z ichiga olgan, himoyasi qonun hujjatlariga muvofiq belgilangan tartibda ta'minlanadigan ma'lumotlarga nisbatan tatbiq etilmaydi.

3. Ushbu yo‘riqnoma axborotlashtirish obyektlarida (axborot tizimlarining ma'lumotlar bazalari, ish stansiyalari tashuvchilari, olinadigan tashuvchilar va boshqalar) saqlanadigan yoki aloqa kanallari orqali uzatiladigan og‘zaki, moddiy va elektron shakldagi konfidensial ma'lumotlarning saqlanishini ta'minlash tartibini belgilaydi.

4. Quyidagi konfidensial ma'lumotlar himoya qilinishi kerak:

Bankning “Xizmatda foydalanish uchun” belgisi bo‘lgan rasmiy (ishga taalluqli) ma'lumotlari, shu jumladan tarqatilishi cheklangan ma'lumotlarni o‘z ichiga olgan hujjatlar, fayllar va nashrlarni hisobga olish, muomalada bo‘lish va saqlash tartibi to‘g‘risidagi yo‘riqnomada belgilangan tarqatilishi cheklangan ma'lumotlar;

uchinchi tomon tashkilotlarining (ariza beruvchilar, yetkazib beruvchilar, mijozlar, hamkorlar va boshqalar) ular bilan o‘zaro hamkorlik qilish jarayonida belgilangan konfidensial ma'lumotlari;

bankning tijorat sirini tashkil etuvchi ma'lumotlar;

bank xodimlarining shaxsiy ma'lumotlari;

ish dunyosidagi axborot tizimlarida foydalaniladigan shaxsiy ma'lumotlar.

5. Ushbu yo‘riqnoma da quyidagi asosiy tushunchalardan foydalaniladi:

konfidensial ma'lumotlarga kirish: ma'lum shaxslarni konfidensial ma'lumotlar bilan uning egasining roziligi bilan yoki boshqa qonuniy asoslarda, ushbu ma'lumotlarning konfidensialligini ta'minlash sharti bilan tanishtirish;

konfidensial ma'lumot: davlat sirlarini tashkil etuvchi ma'lumotlarni o'z ichiga olmagan, foydalanishi qonun hujjatlariga muvofiq cheklangan hujjatlashtirilgan ma'lumotlar;

konfidensial ma'lumotlarni oshkor qilish: har qanday shaklda (og‘zaki, yozma, boshqa shaklda, shu jumladan texnik vositalardan foydalangan holda) konfidensial ma'lumotlar ushbu ma'lumot egasining roziligisiz uchinchi shaxslarga ma'lum bo‘lgan harakat yoki harakatsizlik;

uchinchi shaxs: amaldagi qonunchilikka muvofiq yuridik shaxs hisoblanmaydigan har qanday jismoniy yoki yuridik shaxs yoki xorijiy tashkilot.

6. Bankda konfidensial ma'lumotlarni himoya qilishni tashkil etishning zaruriy sharti bu ma'lumotlarga kirishni cheklash va oshkor qilmaslik (sizib chiqishining oldini olish) hamda konfidensial ma'lumotlarning saqlanishini (yo‘qolishi, yo‘q qilinishi, yaxlitligi o‘zgarishiga yo‘l qo‘ymaslik) ta'minlashdir.

II. Konfidensial ma'lumotni aniqlash tartibi

7. Konfidensial ma'lumotlar ro‘yxatini shakllantirish bo‘yicha ishlarni tashkil etish bank rahbariyati tomonidan amalga oshiriladi.

8. Bankning qog‘oz va elektron shakldagi konfidensial ma'lumotlari, shu jumladan tijorat sirini tashkil etuvchi ma'lumotlar va shaxsiy ma'lumotlar ro‘yxati konfidensial axborotni tashkil etuvchi ma'lumotlar ro‘yxatini aniqlash bo‘yicha komissiya (keyingi o‘rinlarda komissiya) tomonidan belgilanadi.

Komissiya tuziladi va uning tarkibi bank rahbariyatining buyrug‘i bilan belgilanadi.

9. Komissiyaning vazifalariga quyidagilar kiradi:

bank faoliyatining barcha jihatlarini tahlil qilish va bank bosh ofis va AB tomonidan foydalaniladigan ma'lumotlar inventarizatsiyasini o‘tkazish;

inventarizatsiya natijalari bo‘yicha bank konfidensial ma'lumotlari ro‘yxatini aniqlash;

konfidensial ma'lumotlar ro‘yxatini tasdiqlash va amalga oshirish uchun rahbariyatga taqdim etish;

yiliga kamida bir marta konfidensial ma'lumotlar ro‘yxatining dolzarbligini baholab, bank rahbariyatiga ushbu ro‘yxatga o‘zgartirish va qo‘shimchalar kiritish zarurati to‘g‘risida takliflar kiritish.

10. Komissiya o‘z faoliyatida quyidagi hujjatlarga amal qiladi:

“Tijorat siri to‘g‘risida”gi va “Shaxsiy ma'lumotlar to‘g‘risida”gi qonunlar;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2011-yil 7-noyabrdagi “Milliy axborot resurslarini muhofaza qilish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” gi 2011-yil 8-iyuldagi PQ-1572-son qarorini amalga oshirish chora-tadbirlari to‘g‘risida” gi 296-son qarori;

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 16-oktabrdagi 295-son “O‘zbekiston Respublikasi axborotlashtirish obyektlarida konfidensial axborotni saqlashni tashkil etish va xavfsizligini ta'minlash tartibi to‘g‘risidagi nizomni tasdiqlash haqida”gi qarori;

amaldagi boshqa normativ-huquqiy hujjatlar;

bank ustavi.

11. Bankning amaldagi tijorat sirini tashkil qiluvchi va maxfiy ma’lumotlari ro‘yxatiga o‘zgartirish va qo‘shimchalar bank boshqaruv qarori bilan tasdiqlanadi va konfidentsial ma’lumotlar bilan ishlashga mas’ul xodimlarga yetkaziladi.

12. Bankning konfidensial ma'lumotlar ro‘yxatida belgilangan har qanday ko‘rinishdagi konfidensial ma'lumotlar konfidensial saqlanishi va oshkor etilmasligi lozim.

III. Konfidensial ma'lumotlarni himoya qilish bo‘yicha umumiy talablar

13. Bank konfidensial ma'lumotlari ro‘yxatiga kiritilgan konfidensial ma'lumotlar (keyingi o‘rinlarda konfidensial ma'lumotlar deb yuritiladi) bank xodimlari bo‘lmagan uchinchi shaxslarga har qanday shaklda va har qanday ko‘rinishda oshkor etilishi mumkin emas, hamda uchinchi shaxslarning mulkiga aylana olmaydi.

14. Konfidensial ma'lumotlar bank xodimi tomonidan uchinchi shaxslarga faqat bank rahbariyatining roziligi bilan oshkor etilishi mumkin.

15. Konfidensial ma'lumotlar bank rahbariyatining roziligisiz ushbu konfidensial ma'lumotlardan foydalanish huquqiga ega bo‘lmagan bank xodimlariga berilishi va oshkor etilishi mumkin emas.

16. Konfidensial ma'lumotlar Internetda tarqatilishi, ochiq matbuotda, radio va televideniye eshittirishlarida va boshqa ommaviy axborot vositalarida e'lon qilinishi mumkin emas.

17. Konfidensial ma'lumotlar bank nazorat qilinadigan hududda joylashgan lokal tarmoqda qayta ishlanishi mumkin.

18. Konfidensial ma'lumotlarni bank nazorat qilinadigan zonasidan tashqariga, aloqa kanallari orqali uzatishda mazkur yo‘riqnomaning 14-bo‘limida ko‘rsatilgan talablar bajarilishi zarur.

19. Bank rahbariyatining ruxsatisiz fayl tashuvchilarda konfidensial ma'lumotlarni nazorat qilinadigan zonadan tashqariga olib chiqish taqiqlanadi.

20. Bankning axborot tizimlarini va konfidensial ma'lumotlarni himoya qilish bo‘yicha ishlarni tashkil etish va amalga oshirish O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015 yil 16 oktyabrdagi “O‘zbekiston Respublikasi axborotlashtirish obyektlarida konfidensial axborotni saqlashni tashkil etish va xavfsizligini ta'minlash tartibi to‘g‘risidagi nizomni tasdiqlash to‘g‘risida” gi 295-son qarori talablariga muvofiq amalga oshiriladi.

IV. Xodimlar tomonidan konfidensiallikni ta'minlash

21. Bank xodimi faoliyati davomida o‘ziga ma'lum bo‘lgan konfidensial ma'lumotlarni tashkil etuvchi ma'lumotlarni oshkor qilmaslik majburiyatini oladi.

Ushbu talabni bajarish uchun bankning har bir xodimi bilan konfidensial ma'lumotlarni oshkor etmaslik to‘g‘risida shartnoma tuziladi, unda xodim va ish beruvchining tegishli majburiyatlari, shuningdek, konfidensial ma'lumotlar oshkor qilingan taqdirda xodimning javobgarligi belgilab qo‘yiladi.

22. Bank xodimi ishlagan davrida, shuningdek, u bilan mehnat shartnomasi bekor qilingan kundan boshlab kamida 5 (besh) yildan kam bo‘lmagan muddatda Konfidensial ma'lumotlar ro‘yxatiga kiritilgan konfidensial ma'lumotlarni oshkor qilmaslik va ularni tajovuzlardan yoki uchinchi shaxslarga o‘tkazish yoki oshkor qilishga urinishlardan himoya qilishga majburdir..

23. Bank rahbariyati va xodimi o‘rtasida konfidensial ma’lumotlarni oshkor etmaslik to‘g‘risidagi shartnomaning bajarilishi va imzolanishi bank Xodimlarni boshqarish departamenti tomonidan, MBXOda esa – MBXOdagi xodimlarni boshqarish bo‘linmalari tomonidan ta’minlanadi..

24. Bank Xodimlarni boshqarish departamenti va MBXOning Xodimlar bo‘limi xodimini konfidensial ma’lumotlarni oshkor qilganlik uchun javobgarlik to‘g‘risida xabardor qilishi va uni oshkor etmaslik to‘g‘risidagi shartnoma shartlari bilan uni imzolashdan oldin tanishtirishi shart.

V. Kontragentlar tomonidan konfidensiallikni ta'minlash

25. Yuridik va jismoniy shaxslar (keyingi o‘rinlarda kontragentlar) bilan ishlarni bajarish yoki xizmatlar ko‘rsatish bo‘yicha tuzilgan shartnomalar, ular bilan tuzilgan shartnomalar doirasida o‘zaro munosabatlarda har qanday konfidensial ma'lumotlarning chiqib ketishining oldini olish uchun konfidensiallik shartlari ko‘zda tutilishi kerak.

26. Kontragentlar bilan tuzilgan shartnomalarda nazarda tutilgan konfidensiallik shartlari quyidagi talablarni aks ettirishi kerak:

kontragent o‘ziga ma'lum bo‘lgan yoki shartnoma tuzish va/yoki bajarish natijasida ma'lum bo‘ladigan har qanday ma'lumotlar va/yoki ma'lumotlarning konfidensialligini saqlash majburiyatini oladi;

kontragent shartnoma amal qilish muddati davomida va uni bekor qilgandan keyin kamida 5 yil davomida ma'lumotlarning konfidensialligini ta'minlashi kerak.

27. Kontragentlar bilan tuzilgan shartnomalarni bajarish doirasida unga taqdim etiladigan har qanday moliyaviy, iqtisodiy, ishlab chiqarish, texnik va boshqa ma'lumotlarning konfidensialligi ta'minlashi kerak.

28. Agar kontragent bilan tuzilgan shartnomada bankning konfidensial ma'lumotlari ro‘yxatiga kiritilgan ma'lumotlar almashinuvi nazarda tutilgan bo‘lsa, u holda ushbu kontragent shartnomaning ajralmas qismi bo‘lgan Konfidensiallik to‘g‘risidagi shartnomani qo‘shimcha ravishda tuzishi shart.

29. Konfidensiallik to‘g‘risidagi shartnoma taraflarining konfidensial ma'lumotlarni oshkor qilmaslik to‘g‘risidagi majburiyatlarini va ushbu ma'lumotlar uning aybi bilan oshkor qilingan taqdirda kontragentning javobgarligini belgilaydi.

VI. Bank sirini himoya qilishga qo'yiladigan talablar

31. Bankning bank sirini tashkil etuvchi ma’lumotlari bank va uning xodimlari tomonidan himoyalanishi lozim.

32. Bank sirini himoya qilishni ta’minlash uchun bank xodimlari bank tizimida bank sirini himoya qilish to‘g‘risidagi nizom talablariga rioya etishlari shart.

33. Bank sirini tashkil etuvchi ma’lumotlarning himoya qilinishini kafolatlaydi.

Bank rahbarlari va boshqa xodimlariga o‘zlariga ishonib topshirilgan yoki o‘z xizmat vazifalarini bajarishi munosabati bilan ma’lum bo‘lgan bank sirini tashkil etuvchi ma’lumotlarni oshkor qilish, shuningdek ulardan shaxsiy maqsadlarda yoki uchinchi shaxslar manfaatlarini ko‘zlab foydalanish taqiqlanadi, uchinchi shaxslarga bunday foydalanish imkoniyatini bevosita yoki bilvosita taqdim etish, shu jumladan ularni saqlash tartibini buzish natijasida.

34. Bank rahbari yoki boshqa xodimi bank bilan tuzilgan mehnat shartnomasi bekor qilinganidan keyin Bankda ishlagan vaqtida o‘ziga ma’lum bo‘lgan bank sirini tashkil etuvchi ma’lumotlarni oshkor qilishga haqli emas.

Bank sirini tashkil etuvchi ma’lumotlar mijozga (muxbirga), uning vakolatli vakillariga, shuningdek boshqa shaxslarga “Bank siri to‘g‘risida”gi qonunda belgilangan tartibda taqdim etiladi.

35. Bankning bank sirini tashkil etuvchi konfidensial ma’lumotlar bankning konfidensial ma’lumotlari ro‘yxatiga kiritilgan.

36. Bank siri va tijorat siriga oid ma’lumotlar shu jumladan elektron shakldagisi ham ushbu yo‘riqnoma talablariga muvofiq himoya qilinishi kerak.

37. Moddiy tashuvchida bank siri bo‘lgan ma’lumotlar bank tarkibiy bo‘linmalaridagi seyflarda yoki qulflanadigan shkaflarda saqlanishi kerak, ulardan faqat ushbu ma’lumotlarga ruxsat berilgan xodimlar foydalanishi mumkin.

Ushbu ma'lumotlarga yo'l qo'yilgan tarkibiy bo'linmalarning rahbarlari va xodimlari bank siri bo'lgan hujjatlarning konfidensialligini ta'minlash uchun javobgardirlar.

38. Elektron shaklda bank siri bo'lgan ma'lumotlarga, shuningdek moddiy tashuvchida bank siri bo'lgan ma'lumotlarga kirish cheklangan bo'lishi kerak.

Ish stansiyalari va olinadigan tashuvchilarda bank siri bo'lgan ma'lumotlarni saqlash, shuningdek ularni aloqa kanallari orqali uzatish ushbu Yo'riqnomaning 12, 13 va 14-bo'limlari talablariga muvofiq amalga oshirilishi kerak.

VII. Tijorat sirlarini himoya qilish uchun qo‘yiladigan talablar

39. Bankning tijorat siri bank uchun ilmiy-texnikaviy, texnologik, ishlab chiqarish, moliya, iqtisodiy va boshqa sohalarda tijorat ahamiyatiga ega bo‘lgan ma’lumotlardir.

40. Tijorat sirlarini himoya qilishni ta’minlashda bank xodimlari Tijorat sirlari to‘g‘risidagi nizom talablariga rioya etishlari zarur.

41. Bankning tijorat sirini tashkil etuvchi konfidensial ma’lumotlar bankning konfidensial ma’lumotlari ro‘yxatiga kiritilgan.

42. Tijorat siri bo'lgan ma'lumotlar ushbu Yo'riqnoma talablariga muvofiq himoya qilinishi kerak.

43. Xodimlar va pudratchilar ushbu yo‘riqnoma ning 4 va 5-bo‘limlari talablariga rioya qilgan holda bank tijorat siri bo‘lgan ma’lumotlarning konfidensialligini ta’minlashlari shart.

44. Tijorat siri bo‘lgan ma’lumotlar bank rahbariyatining roziligisiz har qanday shaklda (og‘zaki, yozma yoki elektron shaklda) uchinchi shaxslarga oshkor etilishi mumkin emas.

45. Tijorat siri bo'lgan ma'lumotlarning moddiy tashuvchisida ushbu ma'lumotni o'z ichiga olgan hujjatning rekvizitlari "Tijorat siri" deb belgilanishi mumkin.

Moddiy tashuvchidagi tijorat siri bo‘lgan hujjatlar bank tarkibiy bo‘linmalaridagi seyflarda yoki qulflanadigan shkaflarda saqlanishi kerak, ulardan faqat ushbu ma’lumotlarga ruxsat berilgan xodimlar foydalanishi mumkin.

Tijorat siri bo'lgan hujjatlarning konfidensialligini ta'minlash uchun ushbu ma'lumotlarga yo'l qo'yilgan tarkibiy bo'linmalarning rahbarlari va xodimlari javobgardir.

46. Elektron shaklda tijorat siri bo'lgan ma'lumotlarga, shuningdek moddiy tashuvchida tijorat siri bo'lgan ma'lumotlarga kirish cheklangan bo'lishi kerak.

Tijorat siri bo'lgan ma'lumotlarni ish stansiyalari va olinadigan tashuvchilarda saqlash, shuningdek ularni aloqa kanallari orqali uzatish ushbu Yo'riqnomaning 12, 13 va 14-bo'limlari talablariga muvofiq amalga oshirilishi kerak.

47. Tijorat siri bo‘lgan hujjatlar, shuningdek elektron shakldagi tijorat siri bo‘lgan ma’lumotlar boshqa tarkibiy bo‘linmalarning xodimlariga yoki uchinchi shaxslarga tanishtirish uchun faqat bank rahbariyatining ruxsati bilan yoki belgilangan tartibda berilishi mumkin. qonun bilan belgilangan. aks holda, ushbu shaxslarga ushbu ma'lumotlarni taqdim etish tijorat sirini oshkor qilish deb hisoblanadi.

VIII. Shaxsiy ma'lumotlarni himoya qilish talablari

48. Bankning himoyalangan shaxsiy ma’lumotlari bankning jismoniy shaxslar bo‘lgan xodimlari, mijozlari yoki kontragentlariga tegishli ma’lumotlar yoki xodim, mijoz yoki kontragent-jismoniy shaxsni aniqlash imkonini beruvchi ma’lumotlardir.

49. Bankning shaxsiy ma’lumotlari elektron, qog‘oz yoki boshqa moddiy axborot tashuvchida qayd etilishi mumkin.

50. Bank xodimlarining shaxsiy ma’lumotlarini qayta ishlash, tizimlashtirish, hisobga olish, saqlash va himoya qilishni Xodimlar bilan ishlash departamenti va MBXOda xodimlar boshqaruvi bo‘linmalari ta’minlashi kerak.

Bank mijozlarining shaxsiy ma’lumotlariga ishlov berish, tizimlashtirish, hisobga olish, saqlash va xavfsizligini ta’minlash bankning tarkibiy bo‘linmalari va mijozlar bilan ishlovchi xodimlari, shuningdek, bankning axborot bank tizimlari tomonidan amalga oshiriladi.

51. Bank shaxsiy ma’lumotlarning xavfsizligi shaxsiy ma’lumotlarning yo‘q qilinishi, o‘zgartirilishi, bloklanishi, ko‘chirilishi, tarqatilishiga olib kelishi mumkin bo‘lgan ruxsat etilmagan, shu jumladan tasodifiy kirishni, shuningdek, ruxsat etilmagan boshqa harakatlarni bartaraf etishga qaratilgan.

52. Bankning shaxsiy ma’lumotlarga kirish huquqiga ega bo‘lgan Xodimlar bilan ishlash departamenti va MBXOda boshqa xodimlari shaxsiy ma’lumotlarning konfidensialligini ta’minlashlari shart – shaxsning shaxsiy ma’lumotlarini uning roziligisiz yoki boshqa shaxslarga oshkor qilmasliklari yoki tarqatmasliklari shart.

53. Bankning himoyalangan shaxsiy ma’lumotlari bankning konfidensial ma’lumotlari ro‘yxatiga kiritilishi va ushbu yo‘riqnoma talablariga muvofiq himoya qilinishi lozim.

IX. Xodimlarga konfidensial ma'lumotlarga kirishga ruxsat berish tartibi

54. Bankning konfidensial ma’lumotlariga ishlov berish, saqlash va ulardan foydalanish Bankning ushbu konfidensial ma’lumotlarga kirish huquqiga ega bo‘lgan xodimlari tomonidan amalga oshirilishi kerak.

55. bankning konfidensial ma’lumotlarga yo‘l qo‘yilgan xodimlarining ro‘yxati bank rahbariyati tomonidan belgilanadi va bu xodimlar bankning konfidensial ma’lumotlar ro‘yxatida har bir ro‘yxatida ko‘rsatilishi shart.

56. Bank boshqa xodimlarining unga kiritilmagan va konfidensial ma’lumotlar ro‘yxatida ko‘rsatilmagan konfidensial ma’lumotlariga kirishga va ular bilan tanishishga bank rahbariyatining ruxsati bilangina yo‘l qo‘yiladi.

57. Konfidensial ma'lumotlar qayta ishlanadigan binolarga, konfidensial ma'lumotlar moddiy tashuvchida saqlanadigan seyflar va shkaflarga, ish stansiyalariga, olinadigan tashuvchilarga va konfidensial ma'lumotlar elektron shaklda saqlanadigan va qayta ishlanadigan axborot tizimlariga kirish konfidensial ma'lumotlar faqat vakolatli xodimlar tomonidan amalga oshiriladi.

X. Konfidensial ma'lumotlar qayta ishlanadigan binolarga qo'yiladigan talablar

58. Bank tomonidan konfidensial ma’lumotlarga ishlov beriladigan va saqlanadigan binolar ro‘yxati (keyingi o‘rinlarda himoya qilinadigan binolar deb yuritiladi) hujjatlashtiriladi.

59. Himoya qilinadigan binolarga bankning 2 va 3-zonadagi tarkibiy bo‘linmalarining ofis binolari, shu jumladan asosiy va zaxira ma’lumotlarni qayta ishlash markazlarining server xonalari (keyingi o‘rinlarda MQIM deb yuritiladi) kiradi - axborot tizimining ma’lumotlar bazasi serverlarini joylashtirish konfidensial ma’lumotlarni qayta ishlash va saqlash, shuningdek bank rahbariyati uchun majlislar zali.

60. Ushbu yo‘riqnoma ning 59-bandida ko‘rsatilgan bank qo‘riqlanadigan binolariga ruxsat etilmagan shaxslarning ruxsatsiz kirishiga yo‘l qo‘yilmaydi.

Bank qo‘riqlanadigan binolarida ruxsat etilmagan shaxsning bo‘lishi faqat uning hamrohligida yoki bank xodimining mavjudligi bilan mumkin.

61. Himoya qilinadigan binolarga nisbatan, ularga ruxsat etilmagan shaxslarning nazoratsiz kirishini, shuningdek, ularda qayta ishlangan va saqlanadigan konfidensial ma'lumotlarga ruxsatsiz kirishni oldini olish uchun quyidagi choralar ko'rilishi kerak:

hodisalar oralig'ida va ishlamaydigan vaqtlarda himoyalangan binolarning eshiklari kalit bilan qulflangan bo'lishi kerak, bunda kalitlar ularda ishlaydigan yoki ushbu binolar uchun mas'ul shaxslarga beriladi;

qo'riqlanadigan binolarda ishlamaydigan vaqtlarda yoqilgan o'g'irlik signalizatsiya datchiklari, shu jumladan hujumni aniqlash sensori o'rnatilishi kerak;

koridorlarga videokuzatuv kameralari o'rnatilishi kerak, ularning ko'rib chiqilishi qo'riqlanadigan binolarga kirishni qamrab olishi kerak;

matn va grafik konfidensial ma'lumotlarni derazalar orqali ko'rishni istisno qilish uchun himoyalangan binolar tegishli vositalar bilan jihozlangan bo'lishi kerak (pardalar yoki pardalar);

qo'riqlanadigan binolarning yong'in va xavfsizlik signalizatsiyasi tizimi faqat ma'lumot to'plash uchun simli sxema bo'yicha qurilgan (boshqaruv paneli bilan ulanish) va himoyalangan binolar bilan bir xil nazorat qilinadigan zonada joylashgan;

himoyalangan binolardagi jismoniy tashuvchilar haqidagi konfidensial ma'lumotlar seyflarda yoki qulflanadigan shkaflarda saqlanishi kerak.

3-zonaning qo'shimcha himoyalangan binolari kirish joyidagi temir eshiklar va biometrik ma'lumotlarga asoslangan kirishni boshqarish va boshqarish tizimi (keyingi o'rinlarda ACS) bilan jihozlangan bo'lishi kerak.

62. Uskunalarni, mebellarni o'rnatish, ta'mirlash va almashtirish, qo'riqlanadigan binolarda ta'mirlash bank rahbariyati bilan kelishilgan holda va bank tarkibiy bo'linmasi xodimi nazorati ostida amalga oshiriladi. 3-zonaning qo'riqlanadigan binolari - Xavfsizlik va axborotlarni muhofaza qilish departamenti nazorati ostida.

63. Bankning qo‘riqlanadigan binolarida, xususan, majlislar zalida maxfiy tadbirlarni o‘tkazish vaqtida bino ichida mobil qurilmalar, audio va video qayd etish vositalaridan foydalanish taqiqlanadi.

64. Bank asosiy va zaxira ma’lumotlarni qayta ishlash markazlarining server xonalariga nisbatan quyidagi qo‘shimcha talablar bajarilishi kerak:

u yerda o'rnatilgan uskunaga texnik xizmat ko'rsatish uchun ishlaydigan shaxslarni server binolariga qabul qilish ruxsat berish tizimida belgilangan tartibda amalga oshirilishi kerak;

server xonalariga faqat ro'yxati Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan belgilanadigan xodimlarga ruxsat beriladi;

server xonalarida zarur profilaktika va ta’mirlash ishlarini bajarish uchun boshqa shaxslarni qabul qilish faqat Xavfsizlik va axborotlarni muhofaza qilish departamenti direktorining ruxsati bilan amalga oshirilishi mumkin;

biometrik ma'lumotlarga asoslangan kirishni boshqarish tizimini o'rnatish bilan server xonasining eshigi temir bo'lishi kerak.

65. Ushbu Yo'riqnomaning ushbu bo'limida ko'rsatilgan himoyalangan binolarni ruxsatsiz kirishdan himoya qilish talablarini tashkil etish va ta'minlash uchun javobgarlik Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori zimmasiga yuklanadi.

XI. Axborot tizimlarida konfidensial ma'lumotlarni himoya qilishga qo‘yiladigan talablar

66. Bankning konfidensial ma’lumotlarni qayta ishlovchi axborot tizimlari va resurslariga quyidagilar kiradi:

Bankning avtomatlashtirilgan bank tizimi (keyingi o‘rinlarda ABT deb yuritiladi) va ABT ma’lumotlar bazasi;

Internet-Banking va mobil Banking tizimlari va ularning ma'lumotlar bazalari;

CRM, DWH, CROBS, ELMA BPM va SAP axborot tizimlari va ularning ma'lumotlar bazalari;

ERI elektron hujjat aylanishi tizimi va uning ma'lumotlar bazasi;

SWIFT Banklar o'rtasida moliyaviy xabarlarni uzatish tizimi (keyingi o'rinlarda SWIFT tizimi deb yuritiladi) va bank SWIFT tizimining ma'lumotlar bazasi;

Way4 ishlov berish tizimi va tizim ma'lumotlar bazasi;

bank ERI kalitlarini ro‘yxatdan o‘tkazish markazi ma’lumotlar bazasi.

67. Ma'lumotlar bazasi serverlari va uni himoya qilish vositalari himoyalangan binolarda (asosiy va zaxira ma'lumotlarni qayta ishlash markazlarining server binolari)

joylashgan bo'lishi kerak, ularga kirish xodimlar va ruxsatsiz shaxslar uchun cheklangan.

68. Axborot tizimlarida konfidensial ma'lumotlarni himoya qilish uchun quyidagi chora-tadbirlar majmuini nazarda tutuvchi axborotni himoya qilish tizimi qo'llanilishi kerak:

bank axborot xavfsizligi siyosatiga 7-ilovada keltirilgan parolni himoyalash va autentifikatsiya qilish bo‘yicha yo‘riqnomaga muvofiq foydalanuvchilarning axborot tizimiga kirishini login va parol hamda boshqa identifikatorlar asosida tabaqalashtirish;

tarmoq infratuzilmasi darajasida axborot xavfsizligi va tarmoqlararo ekran to'g'risidagi nizomga muvofiq axborot tizimlari ma'lumotlar bazasi serverlarini tashqi tarmoqqa va korporativ tarmoqqa ulashda tarmoqlararo ekran va IDPS hujumlarini aniqlash va oldini olish vositalaridan foydalangan holda tarmoqqa ruxsatsiz kirish, tarmoqqa kirish va hujumlardan himoya qilish. Bank Axborot xavfsizligi siyosatiga 2-ilovasida keltirilgan;

bank Axborot xavfsizligi siyosatiga 8-ilovada keltirilgan virusga qarshi himoya qilish bo‘yicha yo‘riqnomaga muvofiq zararli dasturlardan himoya qilish;

foydalanuvchilarni axborot tizimlariga ulashda, shuningdek administratorlarni tizimlarning server uskunalariga masofadan ulashda xavfsiz ulanishlarni tashkil etish;

ma'lumotlar bazasi serverlarini bron qilish, ma'lumotlarni zaxiralash va axborot tizimlarini arxivlash;

kafolatlangan elektr ta'minoti va aloqani ta'minlash.

69. Profilaktika va ta'mirlash ishlari, zaxiralash va arxivlash, sozlash va kirishni boshqarish uchun axborot tizimining server uskunasiga jismoniy va masofaviy kirish texnik xizmat ko'rsatuvchi ayrim xodimlarga (keyingi o'rinlarda axborot tizimlari administratori deb yuritiladi) taqdim etiladi.

70. Axborot tizimlari administratorining axborot tizimining server uskunasiga masofadan kirishi faqat administratorga ma’lum bo‘lishi va ruxsat etilmagan shaxslarga berilmasligi kerak bo‘lgan parol yordamida amalga oshiriladi. Administrator paroliga qo‘yiladigan talablar va uni o‘zgartirish bank axborot xavfsizligi siyosatida belgilangan.

71. Axborot tizimlarida konfidensial ma'lumotlarning himoya qilinishini ta'minlash uchun administratori quyidagilarga majburdir:

axborot tizimlari ma’lumotlar bazasida saqlanayotgan ma’lumotlarni uchinchi shaxslarga tarqatmaslik;

axborot tizimlarining ma'lumotlar bazasida saqlanadigan ma'lumotlarning nusxalarini yaratmaslik, agar bu ma'lumotlarni zaxiralash va arxivlash tadbirlarida nazarda tutilmagan bo'lsa;

axborot tizimlari ma’lumotlar bazasida saqlanayotgan ma’lumotlarning nusxalarini ma’lumotlarni zaxiraviy va elektron arxivlar saqlash uchun mo‘ljallanmagan joylarda saqlamaslik.

72. Axborot tizimlarining zaxiraviy ma'lumotlari va elektron arxivlari 3-zonaning qo'riqlanadigan binolarida saqlanishi kerak.

73. PAM imtiyozli foydalanuvchilarni boshqarish tizimi yordamida va ma'lumotlar bazasini boshqarish tizimlari (keyingi o'rinlarda MBBT) orqali axborot tizimi administratorining axborot tizimining ma'lumotlar bazalariga kirishda harakatlarini nazorat qilish va hisobga olish amalga oshirilishi kerak. Jurnal ma'lumotlari kamida bir yil davomida saqlanishi kerak.

PAM tizimi orqali uning ruxsat beruvchi murojaatlari va ma'lumotlar bazasi bilan xatti-harakatlari monitoring qilinishi, shuningdek, ma'lumotlar bazasidan ma'lumotlarning sizib chiqishi holatlarini tekshirishda ruxsat berilmagan harakatlar aniqlanishi kerak. Ushbu nazorat vaqti-vaqti bilan Xavfsizlik va axborotlarni muhofaza qilish departamentining alohida xodimi tomonidan yoki ma'lumotlarning sizib chiqishi holatlarini tekshirish davrida amalga oshirilishi kerak.

74. Axborot tizimlarining server uskunalarida profilaktika va ta'mirlash ishlari Xavfsizlik va axborotlarni muhofaza qilish departamenti direktorining ruxsati bilan amalga oshirilishi kerak.

75. Axborot tizimlari administratori ishdan bo'shatilganda kirish parollarini zudlik bilan o'zgartirish choralari ko'riladi.

76. Axborot tizimlarida ma'lumotlarni qayta ishlashning texnologik jarayonida, shu jumladan nusxalar va arxiv ma'lumotlarini saqlash uchun foydalaniladigan barcha ommaviy axborot vositalari hisobga olinadi. Ushbu yozuv Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan yuritiladi.

Ruxsatsiz shaxslarning ko'rsatilgan ommaviy axborot vositalariga kirishi cheklangan bo'lishi kerak.

XII. Konfidensial ma'lumotlarni elektron shaklda saqlash, qayta ishlash va uzatishga qo‘yiladigan talablar

77. Bankning konfidensial ma’lumotlar ro‘yxatiga kiritilgan konfidensial ma’lumotlar, “Xizmatda foydalanish uchun” belgisi bilan belgilangan ma’lumotlar bundan mustasno, elektron shaklda saqlanishi mumkin.

78. Bankning unga qabul qilingan xodimlari konfidensial ma’lumotlarni elektron shaklda qayta ishlash va saqlash uchun ruxsatga ega.

79. Bank axborot tizimlari tarkibiga kirmaydigan elektron shakldagi konfidensial ma’lumotlar Bankka tegishli bo‘lgan ish stansiyalari va buxgalteriya hisobining olinadigan tashuvchilarida saqlanishi mumkin. Belgilangan ish stansiyalari va buxgalteriya olinadigan vositalar himoya qilinadigan hududlarda joylashgan bo'lishi kerak.

80. Konfidensial ma'lumotlarni elektron shaklda saqlashga yo'l qo'yilmaydi:

fayl serveri, shuningdek ish stansiyalaridagi umumiy tarmoq papkalarida;

xodimga yoki Bankka tegishli har qanday mobil qurilmalar, shu jumladan qayd etish noutbuklari;

bankning ro‘yxatdan o‘tmagan olinadigan tashuvchisi va bank xodimiga tegishli bo‘lgan olinadigan tashuvchi;

bulutli xizmatlar.

81. Konfidensial ma'lumotlarni, xususan, bank va tijorat siri bo'lgan ma'lumotlarni yoki bank shaxsiy ma'lumotlarini saqlaydigan ish stansiyalari quyidagi talablarga javob berishi kerak:

ish stansiyasiga kirish har oyda kamida bir marta o'zgartirilishi kerak bo'lgan parol bilan amalga oshirilishi kerak va parolning murakkabligi Parolni himoya qilish va autentifikatsiya qilish bo'yicha Yo'riqnomaning 7-ilovasida keltirilgan talablarga javob berishi kerak. Bankning axborot xavfsizligi siyosati;

ish stansiyalari, agar foydalanuvchi 5 daqiqa davomida faol bo'lmasa, ekranni avtomatik ravishda blokirovka qilish va uyqu rejimiga o'tish uchun - 20 daqiqa, qulfdan chiqish va uyqu rejimidan chiqishda kirish paroli yordamida amalga oshirilishi kerak;

ish stansiyasiga kirish paroli faqat uning xodimiga ma'lum bo'lishi kerak;

elektron shakldagi konfidensial ma'lumotlar ishchi stansiyaning qattiq diskka kirishda topish qiyin bo'lgan papkalarda va operatsion tizim o'rnatilgan mahalliy diskdan alohida saqlanishi kerak;

konfidensial ma'lumotlarni elektron ko'rinishda ishchi stansiyaning ish stoli va umumiy papkalarida saqlashga yo'l qo'yilmaydi;

ish stansiyasi Bankda foydalanish uchun litsenziyalangan standart dasturiy ta'minot to'plami, shuningdek, virusga qarshi himoya bilan jihozlangan bo'lishi kerak.

82. Konfidensial ma'lumotlarni saqlaydigan ish stansiyalarining jihozlari yoki dasturiy ta'minotidagi har qanday o'zgartirishlar ruxsat etilgan bo'lishi va Axborot texnologiyalari departamenti bilan kelishilgan bo'lishi kerak.

83. Konfidensial ma'lumotlarni elektron shaklda saqlaydigan va qayta ishlovchi ish stansiyalari Internetga ulanmaganligi ma'qul. Shuningdek, ushbu ish stansiyalarini simsiz Wi-Fi tarmog'iga, shu jumladan nazorat qilinadigan hududda tashkil etilganlarga ulashga ruxsat berilmasligi kerak.

84. "Xizmatda foydalanish uchun" yorlig'i bilan ish stansiyasida tayyorlangan konfidensial ma'lumotlar chop etilgandan va ishlov berilgandan so'ng (imzolash va sozlash tafsilotlari) yo'q qilinishi kerak. "Xizmatda foydalanish uchun" belgisi bo'lgan ma'lumotlarni elektron shaklda ish stansiyalarida va har qanday olinadigan tashuvchilarda saqlashga yo'l qo'yilmaydi.

85. Ish stansiyasida har qanday konfidensial ma'lumotlarni, shu jumladan "Xizmatda foydalanish uchun" ni qayta ishlashda xodim uchinchi shaxslarning monitor ekranlaridan matn va grafik konfidensial ma'lumotlarni ko'rishiga yo'l qo'ymaslik choralarini ko'rishi kerak.

86. Agar konfidensial ma'lumotlarni saqlaydigan ish stansiyasini ta'mirlash zarur bo'lsa, uchinchi tomon tashkilotlar ta'mirlashni boshlashdan oldin ma'lumot saqlovchi va tashuvchi qurilmalarni (HDD) olib tashlashlari kerak. Ma'lumot saqlovchi va tashuvchi qurilmalar ta'mirlash mumkin bo'lmagan hollarda, bu ta'mirlash Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimlari tomonidan nazorat qilinishi kerak.

87. Konfidensial ma'lumotlarni elektron shaklda uzatish bank xodimlari o'rtasida nazorat qilinadigan hudud doirasida mahalliy tarmoq orqali yoki olinadigan tashuvchida amalga oshirilishi kerak.

88. "Xizmatdan foydalanish uchun" belgisi bilan elektron shakldagi konfidensial ma'lumotlar faqat nazorat qilinadigan hududda va faqat olinadigan tashuvchida yoki qog'oz shaklida uzatilishi kerak.

Konfidensial ma'lumotlarni "Xizmatda foydalanish uchun" belgisi bilan elektron shaklda lokal va korporativ tarmoqlar va tashqi tarmoqlarning aloqa kanallari, shuningdek korporativ elektron pochta va messenjer orqali o'tkazish taqiqlanadi.

"Xizmatda foydalanish uchun" belgisi bo'lgan konfidensial ma'lumotlar ushbu yo'riqnoma ning 15-bo'limida belgilangan talablarga rioya qilgan holda nazorat qilinadigan hududdan tashqariga uzatilishi va tarqatilishi kerak.

89. Konfidensial ma'lumotlar elektron shaklda ro'yxatdan o'tmagan ma'lumot tashuvchiga o'tkazilgan taqdirda, u o'tkazilgandan keyin uni tashuvchida o'chirish yo'li bilan yo'q qilinishi kerak.

90. Konfidensial ma'lumotlarni elektron shaklda uzatishda, "Xizmatda foydalanish uchun" belgisi bo'lgan konfidensial ma'lumotlar bundan mustasno, nazorat qilinadigan hudud ichidagi va undan tashqaridagi aloqa kanallari orqali ushbu yo'riqnoma ning 14-bo'limi talablariga rioya etilishi kerak.

91. Bank xodimi, bankning konfidensial ma'lumotlarni saqlaydigan va uzatuvchi elektron shaklda qayta ishlash mobaynida quyidagi talablarga javob berishi kerak:

ish stansiyasiga kirish uchun parolni hech kimga aytmaslik;

Axborot texnologiyalari departamentining roziligisiz ishchi stansiyaning apparat konfiguratsiyasi va dasturiy ta'minot sozlamalarini o'zboshimchalik bilan o'zgartirish taqiqlanadi;

har hafta ish stolidagi papkalarni tekshirish, "Xizmat foydalanish uchun" belgisi bilan elektron shakldagi konfidensial ma'lumotlarni yoki foydalanishda keraksiz bo'lib qolgan boshqa konfidensial ma'lumotlarni aniqlash va yo'q qilish;

ishdan bo'shatilgandan so'ng, Xavfsizlik va axborotlarni muhofaza qilish departamentiga ish stansiyasida konfidensial ma'lumotlar saqlanadigan joy haqida xabar berish shuningdek, konfidensial ma'lumotlarga ega bo'lgan barcha ma'lumot tashuvchi vositalarini qayd etish uchun unga topshirish.

XIII. Konfidensial ma'lumotlarni xizmat doirasida foydalanish uchun hisobga olish, foydalanish va saqlashga qo'yiladigan talablar

92. Elektron shakldagi konfidensial ma'lumotlar hisobga olinadigan ma'lumotlarni tashuvchilarda saqlanishi kerak.

93. Konfidensial ma'lumotlarni saqlash uchun foydalaniladigan hisobga olinadigan tashuvchilar Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan hisobga olinadigan tashuvchilar, mobil qurilmalar, ma'lumotlar saqlash vositalar bilan ishlashda xavfsizlikni ta'minlash bo'yicha bank Axborot xavfsizligi siyosati yo'riqnoma talablariga muvofiq hisobga olinadi.

94. Konfidensial ma'lumotlarni o'z ichiga olgan olinadigan tashuvchilar foydalanilmayotganda seyfda yoki 3-zonaning himoyalangan hududlarida qulflanadigan shkaflarda saqlanishi kerak.

95. Konfidensial ma'lumotlarni saqlash uchun foydalaniladigan olinadigan tashuvchini nazorat qilinadigan hududdan tashqariga olib chiqishga yo'l qo'yilmaydi.

96. Konfidensial ma'lumotlarni saqlash uchun foydalaniladigan hisobga olinadigan tashuvchilar rangli stiker (stiker) bilan belgilanishi va Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan inventarizatsiya qilinishi kerak.

Ommaviy axborot vositalarini va ulardagi belgilar mavjudligini tekshirish Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan kamida olti oyda bir marta amalga oshiriladi.

97. Konfidensial ma'lumotlarga ega bo'lgan hisobga olinadigan tashuvchilardan foydalanishda bank xodimlari quyidagi talablarga rioya qilishlari kerak:

ulardan maqsadli va faqat xizmat vazifalarini bajarish uchun foydalanish;

ushbu Yo'riqnomaning ushbu bo'limi talablari buzilganligi haqidagi har qanday faktlar to'g'risida Xavfsizlik va axborotlarni muhofaza qilish departamentini xabardor qilish;

olinadigan saqlash vositalarining yo'qolishi (o'g'irlanishi) yoki ishlamay qolishi faktlari to'g'risida Xavfsizlik va axborotlarni muhofaza qilish departamentini xabardor qilish;

hisobga olinadigan saqlash vositalarining jismoniy xavfsizligini barcha oqilona vositalar bilan ta'minlash;

hisobga olinadigan vositalarni boshqa shaxslarga bermang.

98. Konfidensial ma'lumotlarga ega qayd hisobining olinadigan tashuvchilaridan foydalanganda, bank xodimlariga, agar ularning jismoniy xavfsizligini ta'minlash choralari ko'rilmasa, ularni qarovsiz qoldirish taqiqlanadi.

99. Bank xodimi ishdan bo‘shatilgan yoki boshqa ish joyiga o‘tkazilgan taqdirda, unga konfidensial ma’lumotlar bilan taqdim etilgan olib qo‘yiladigan tashuvchilar Xavfsizlik va axborotlarni muhofaza qilish departamentiga topshiriladi.

100. Konfidensial ma'lumotlarni o'z ichiga olgan o'chirilgan yoki yo'q qilinishi mumkin bo'lgan hisobga olinadigan ma’lumotlar axborot vositalari qulflanadigan shkaflar yoki seyflarda saqlanishi kerak.

101. Konfidensial ma'lumotlarga ega bo'lgan olinadigan tashuvchilarni foydalanishdan chiqarish to'g'risida qaror qabul qilingandan so'ng, ularni yo'q qilish (utilizatsiya qilish) tartibi yo'q qilish dalolatnomasini tuzish bilan amalga oshirilishi kerak.

102. Keyinchalik foydalanish uchun yaroqsiz bo'lgan konfidensial ma'lumotlarga ega hisobga olinadigan tashuvchilarni utilizatsiya qilishda ular jismoniy yo'q qilinishi kerak. Axborot vositalarini jismoniy yo'q qilish undan qolgan ma'lumotlarni o'qishga imkon bermasligi kerak, buning uchun barcha mikrosxemalarni bolg'a bilan yo'q qilish kerak.

103. Ko'chma tashuvchidan konfidensial ma'lumotlarni o'chirishda ushbu qurilmalarda saqlangan ma'lumotlar kerakli ma'lumotlarni o'chirish va barcha ma'lumotlarni o'chirishda olinadigan tashuvchini formatlash orqali yo'q qilinishi kerak.

XIV. Aloqa kanallari orqali konfidensial ma'lumotlarni uzatishga qo'yiladigan talablar

104. AKHdan foydalanmasdan aloqa kanallari orqali konfidensial ma'lumotlar lokal va korporativ tarmoq orqali boshqariladigan hududda uzatilishi mumkin, bundan "Xizmatda foydalanish uchun" belgisi bo'lgan konfidensial ma'lumotlar bundan mustasno.

105. Nazorat qilinadigan hudud doirasida konfidensial ma'lumotlar Banklararo elektron pochta yoki EHAT tizimi orqali uzatilishi mumkin.

106. Bankning konfidensial ma’lumotlarini, shu jumladan “Xizmat foydalanish uchun” shtampini quyidagi tashqi aloqa kanallari orqali o‘tkazish taqiqlanadi:

elektron pochta orqali va Internetda, shu jumladan Internet pochta xizmatlari (mail.ru, yandex.ru va boshqalar), ijtimoiy tarmoqlar;

tezkor xabar almashish tizimlari orqali;

tashqi himoyalanmagan elektron hujjat aylanish tizimlari.

107. Bank va tijorat siri bo‘lgan konfidensial ma’lumotlar, bankning shaxsiy ma’lumotlari tashqi aloqa kanallari orqali AKHdan foydalanmasdan, faqat bank rahbariyatining ruxsati bilan, u bilan kelishilgan holda uzatilishi mumkin. uni uzatish usuli, masalan, korporativ elektron pochta orqali, va hokazo.

108. Tijorat siri bo'lgan konfidensial ma'lumotlarni uchinchi tomon tashkiloti (kontragent) bilan ular bilan tuzilgan shartnomalar (kontraktlar) doirasida ayirboshlashda, ushbu ma'lumotlarni uzatish usuli shartnomada (s kontraktda) ko'rsatilishi va himoya qilinishi kerak.

109. Bankning “Xizmatdan foydalanish uchun” belgisi bo‘lgan konfidensial ma’lumotlarini uchinchi shaxslar bilan faqat E-xat himoyalangan elektron pochta tizimi orqali yoki elektron pochta orqali, AKH konfidensial ma’lumotlari fayllarini shifrlash sharti bilan almashishga ruxsat etiladi.

110. Bankning konfidensial ma’lumotlarini shifrlash uchun foydalaniladigan AKH belgilangan tartibda sertifikatlangan bo‘lishi kerak.

XV. Konfidensial ma'lumotlarni rasmiy foydalanish uchun hisobga olish, aylanishi va saqlash

111. Rasmiy foydalanish uchun konfidensial ma'lumotlar quyidagilarni o'z ichiga oladi:

Bankning “Xizmat foydalanish uchun” belgisi bilan kiruvchi, chiquvchi va ichki hujjatlari;

O‘zbekiston Respublikasining - Davlat sirlarini himoya qilish masalalari bo‘yicha idoralararo komissiyaning Raisi Bosh vazir o‘rinbosari tomonidan 2006 yil 5 dekabrda tasdiqlangan, tarqatilishi cheklangan ma’lumotlarni o‘z ichiga olgan hujjatlar, ishlar va nashrlarni hisobga olish, muomalada bo‘lish va saqlash tartibi to‘g‘risidagi yo‘riqnomada belgilangan ruxsati cheklangan ma’lumotlarni o‘z ichiga olgan hujjatlar, ishlar va nashrlar;

112. Konfidensial ma'lumotlarning rasmiy foydalanish uchun hujjatlarida "Xizmatda foydalanish uchun" muhri va nusxasining raqami bo'lishi kerak.

113. "Xizmatda foydalanish uchun" muhrini qo'yish zarurligini aniqlash hujjatga - ijrochi va hujjatni imzolagan shaxs tomonidan amalga oshiriladi.

114. Bank boshqaruvi Raisi bank tomonidan tayyorlangan hujjatlardan “Xizmatda foydalanish uchun” muhri olib tashlashga haqli.

115. Bank boshqaruvi va uning tarkibiy bo‘linmalari rahbarlari rasmiy foydalanish uchun hujjatlarning to‘g‘ri hisobi, saqlanishi, ko‘paytirilishi va ishlatilishini ta’minlash uchun javobgardirlar.

116. Hujjatlarni hisobga olish, saqlash, ko‘paytirish va xizmat maqsadlarida foydalanish uchun foydalanilishini nazorat qilish bankning Ijro nazorati departamenti, shuningdek, MBXOdagi idora bo‘linmalariga yuklatilgan.

117. Bankning rasmiy foydalanish uchun hujjatlar bilan ishlash bilan bog‘liq xodimlari ushbu yo‘riqnoma va tarqatilishi cheklangan konfidensial ma’lumotlarni o‘z ichiga olgan hujjatlar, holatlar va nashrlarni hisobga olish, muomalada bo‘lish va saqlash tartibi to‘g‘risidagi yo‘riqnoma bilan tanishishlari shart.

118. Bankning xizmat maqsadlarida foydalanish uchun hujjatlar bilan ishlashga qabul qilingan xodimlariga, agar bu rasmiy zaruratdan kelib chiqmasa, rasmiy

foydalanish uchun hujjatlardagi ma’lumotlarni og‘zaki yoki yozma ravishda begonaga yetkazishi taqiqlanadi.

119. Hujjatlarni rasmiy foydalanish uchun qabul qilish, hisobga olish va saqlash bank Departamenti tomonidan konfidensial bo‘lmagan tarqatilishi mumkin bo‘lgan ma’lumotlarni o‘z ichiga olgan hujjatlar, ishlar va nashrlarni hisobga olish, muomalada bo‘lish va saqlash tartibi to‘g‘risidagi yo‘riqnomaga muvofiq amalga oshiriladi.

120. Bank tarkibiy bo‘linmalarida joylashgan qog‘ozdagi rasmiy foydalanish uchun hujjatlar seyf yoki qulflanadigan shkaflarda saqlanishi kerak.

121. Bank tarkibiy bo‘linmalarida joylashgan qog‘ozda rasmiy foydalanish uchun hujjatlardan foydalanilmagan taqdirda, ular bank Ijro nazorati departamentiga yoki MBXO devonxonasiga topshirilishi mumkin.

122. Hujjatlarni rasmiy foydalanish uchun qabul qilish, hisobga olish (ro'yxatga olish) Ijro nazorati departamenti xodimlari, shuningdek MBXOdagi devona bo'linmalari tomonidan hujjatlarni hisobga olish, muomalada bo'lish va saqlash tartibi cheklangan tarqatiladigan tasniflanmagan ma'lumotlarni o'z ichiga olgan fayllar va nashrlar to'g'risidagi yo'riqnomaga muvofiq amalga oshirilishi kerak.

123. Bankning rasmiy foydalanish uchun hujjatlarini hisobga olish Ijro nazorati departamenti, shuningdek, MBXOdagi devona bo'limlari tomonidan jurnalda amalga oshiriladi, ularning shakli qayd hisobini yuritish tartibi cheklangan tarqatishning konfidensial bo'lmagan ma'lumotlarini o'z ichiga olgan hujjatlar, fayllar va nashrlarning aylanishi va saqlanishi to'g'risida yo'riqnomada belgilangan.

124. Hujjatlarni rasmiy foydalanish uchun berish, ko‘paytirish va tarqatish uchun javobgarlik bank rahbariyati va uning tarkibiy bo‘linmalari zimmasiga yuklanadi.

125. Bank hujjatlarini xizmatda foydalanish uchun tayyorlash bank xodimlari tomonidan xizmatda foydalanish uchun konfidensial ma’lumotlarga ruxsat etilgan ushbu yo‘riqnoma ning 12.5-bandi talablariga javob beradigan ish stansiyalarida va ushbu yo‘riqnoma ning 10-bo‘limi talablariga javob beradi. Bankning qo‘riqlanadigan binolarida amalga oshiriladi.

126. Xizmatda foydalanish uchun bosilgan va imzolangan hujjatlar, ularning loyihalari bilan birgalikda ro'yxatga olish va hisobga olish uchun Ijro nazorati departamenti, shuningdek, MBXO devonxonasiga taqdim etiladi.

127. “Xizmatda foydalanish uchun” belgisi bo‘lgan hujjatlarning elektron nusxalarini ular tayyorlangan va chop etilgandan keyin ish stansiyalari va boshqa elektron tashuvchilarda qoldirish va saqlash taqiqlanadi.

128. Bankda rasmiy foydalanish uchun hujjatlarni ro‘yxatdan o‘tkazish, ko‘paytirish va tarqatish (yuborish) tarqatilishi cheklangan ma’lumotlarni o‘z ichiga olgan hujjatlar, fayllar va nashrlarni hisobga olish, muomalada bo‘lish va saqlash tartibi to‘g‘risidagi yo‘riqnomaga muvofiq amalga oshirilishi kerak.

129. Takrorlangan va ko'paytirilgan hujjatlarni hisobga olish nusxa ko'chirish orqali amalga oshiriladi.

130. Hujjatlarni xizmatda foydalanish uchun respublika hududidagi boshqa tashkilotlarga jo‘natish buyurtma qilingan yoki qimmatli pochta jo‘natmalari, bank kuryerlari yoki E-xat himoyalangan elektron pochta orqali amalga oshiriladi.

Hujjatlarni rasmiy foydalanish uchun xorijiy muassasalar, tashkilotlar va firmalarga o‘tkazishga har bir alohida holatda bank rahbariyatining yozma ruxsati bilan yo‘l qo‘yiladi.

Agar rasmiy foydalanish uchun hujjatlarda boshqa vazirliklar, idoralar va tashkilotlarning vakolatiga kiruvchi ma’lumotlar bo‘lsa, ularni xorijga olib chiqish faqat ushbu vazirliklar, idoralar va tashkilotlarning roziligi bilan amalga oshirilishi mumkin.

131. Xizmatdan foydalanish uchun hujjatlar Ijro nazorati departamenti, shuningdek, MBXO devonxona tomonidan bankning konfidensial ma’lumotlarga yo‘l qo‘yilgan xodimlari foydalanishi uchun beriladi. Ushbu xodimlarning ro'yxati konfidensial ma'lumotlar ro'yxatida belgilanadi.

Xizmatda foydalanish uchun hujjatlarning asl nusxalari bankning Ijro nazorati departamenti, shuningdek, MBXO devonxonasida saqlanadi.

132. Xizmatda foydalanish uchun hujjatlar bank xodimidan Ijro nazorati departamenti, shuningdek, MBXO devonxona bo‘limlari tomonidan qayd hisobi imzo qo‘ygan holda rasmiylashtiriladi va qabul qilinadi. Bu chegaralanmagan tarqatish ma'lumotlarini o'z ichiga olgan hujjatlar, bank fayllar va nashrlarni hisobga olish, aylanish va saqlash tartibi to'g'risidagi yo'riqnomada belgilangan.

133. Bank hujjatidan “Xizmat foydalanish uchun” muhri olib tashlash, rasmiy foydalanish uchun hujjatlarni doimiy saqlash va yo‘q qilish uchun arxivga topshirish Qayd hisobini yuritish, tarqatilishi cheklangan konfidensial ma'lumotlarni o'z ichiga olgan hujjatlar, ishlar va nashrlarni saqlash muomalada bo‘lish tartibi to‘g‘risidagi yo‘riqnomaga muvofiq amalga oshirilishi kerak.

XVI. Konfidensial axborotni himoya qilish talablariga rioya etilishini nazorat qilish

134. Ushbu yo‘riqnoma da belgilangan konfidensial ma’lumotlarni himoya qilish talablariga rioya etilishi ustidan nazorat bank konfidensial ma’lumotlarining saqlanishining amaldagi holatini o‘rganish va baholash, kamchiliklarni va konfidensial ma'lumotlarni himoya qilish bo‘yicha talablarning buzilishini aniqlash maqsadida amalga oshiriladi.

135. Bank tarkibiy bo‘linmalari rahbarlari o‘zlariga bevosita bo‘ysunuvchi xodimlar tomonidan konfidensial ma’lumotlarni himoya qilish bo‘yicha talablarga rioya etilishini doimiy nazorat qilib borishlari shart.

136. Xavfsizlik va axborotlarni muhofaza qilish departamenti mutaxassislari, shuningdek, MBXO Xavfsizlik va axborotni muhofaza qilish bo’limlari konfidensial ma'lumotlarni himoya qilish talablariga muvofiqligini rejali yoki rejadan tashqari tekshirishlarni amalga oshiradilar.

137. Bank Xavfsizlik va axborotlarni muhofaza qilish departamenti hamda MBXO Xavfsizlik va axborotni muhofaza qilish bo’limlari konfidensial ma’lumotlarni himoya qilish maqsadida quyidagilarni tekshirishni ta’minlaydi:

elektron va qog'oz ko'rinishdagi konfidensial ma'lumotlarni saqlash va uzatish talablarini bajarish;

konfidensial ma'lumotlarga ega bo'lgan hisobga olinadigan tashuvchilarni to'g'ri saqlash va ulardan foydalanish;

“Xizmatda foydalanish uchun” deb tasniflangan hujjatlarni saqlash va muomalaga qo‘yish talablariga rioya qilish;

Bank xodimi bilan konfidensial ma’lumotlarni oshkor etmaslik to‘g‘risidagi shartnoma mavjudligi;

pudratchilar bilan tuzilgan shartnomalarga (kontraktlar) konfidensial to'g'risidagi bandlarni yoki konfidensial shartnomalarini kiritish;

konfidensial belgilarini belgilashning to'g'riligi;

bank xodimlarining ushbu yo‘riqnoma talablaridan xabardorligi va boshqalar.

138. Xavfsizlik va axborotlarni muhofaza qilish departamenti va MBXOning Xavfsizlik va axborotni muhofaza qilish bo'limlari mutaxassislari tomonidan konfidensial ma'lumotlarni himoya qilish talablariga rioya qilish bo'yicha rejali tekshiruvlar yiliga kamida bir marta amalga oshiriladi.

139. Tarkibiy bo'linmalarda qo'llaniladigan barcha hujjatlar bilan tanishish, ish stansiyalari va hisobga olinadigan tashuvchilarni tekshirish, shuningdek, tarkibiy bo'linmalar xodimlari bilan suhbatlar va maslahatlar o'tkazish, yozma tushuntirishlar, ma'lumotnomalar, hisobotlarni talab qilish huquqiga ega.

140. Tekshiruvlar natijalari bo'yicha konfidensial ma'lumotlarni himoya qilish holatini, aniqlangan kamchiliklar va buzilishlarni, ularni bartaraf etish bo'yicha takliflarni aks ettiruvchi dalolatnoma tuziladi.

141. Tarkibiy bo'linma rahbari konfidensial ma'lumotlarni himoya qilishda aniqlangan kamchiliklar va buzilishlarni, shuningdek ularning paydo bo'lishiga yordam beradigan sabablar va shartlarni dalolatnomada belgilangan muddatlarda bartaraf etishga majburdir.

142. Konfidensial ma’lumotlar sizib chiqib ketgan yoki oshkor qilingan taqdirda, ko‘rsatilgan voqea sodir bo‘lgan bank tarkibiy bo‘linmasi rahbari bu haqda zudlik bilan Xavfsizlik va axborotlarni muhofaza qilish departamentiga va MBXO axborotni himoya qilish bo’limiga yoki. bank rahbariyatiga xabar beradi.

143. Konfidensial ma’lumotlarning chiqib ketishi yoki oshkor etilishi faktlari bo‘yicha bank rahbariyati ichki tekshiruv tayinlashi mumkin. O‘tkazilgan ichki tekshirish natijalariga ko‘ra, bank rahbariyati tomonidan aybdor shaxslarni javobgarlikka tortish va bunday huquqbuzarliklarning takrorlanishiga yo‘l qo‘ymaslik choralarini ko‘rish yuzasidan tegishli qaror qabul qilinadi.

144. Konfidensial ma'lumotlarning elektron ko'rinishda sizib chiqishi faktlarini nazorat qilish va aniqlash uchun bank ATB DLP konfidensial ma'lumotlar sizib chiqishining oldini olish tizimidan foydalanadi.

XVII. Konfidensial ma'lumotlarni oshkor etmaslik majburiyatlari

145. Bank xodimlari quyidagilarga majburdirlar:

Bankda ishlagan davrda va mehnat shartnomasi bekor qilingan kundan e'tiboran 5 (besh) yil mobaynida konfidensial ma'lumotlarni oshkor qilmaslik, shuningdek, yuqorida ko‘rsatilgan ma'lumotlarni uchinchi shaxslar tajovuzidan yoki ularga o‘tkazish yoki oshkor etishga urinishlardan himoya qilish;

ish jarayonida o‘ziga ma'lum bo‘lgan konfidensial ma'lumotlardan faqat bank manfaatlari yo‘lida foydalanish;

konfidensial ma'lumotlardan shaxsiy maqsadlarda, shu jumladan boshqa tashkilotda ishlash jarayonida (boshqa tashkilot bilan hamkorlik qilish yoki unga xizmat ko‘rsatish) yoki yakka tartibdagi tadbirkor sifatida biznes yuritish jarayonida, ilmiy, pedagogik faoliyatda, ommaviy chiqishlar, intervyu jarayonida foydalanmaslik;

bankning unga ruxsat etilmagan konfidensial ma'lumotlariga kirmaslik;

bankning har qanday konfidensial ma'lumotlariga uchinchi shaxslarning, shuningdek, bank xodimlarining konfidensial ma'lumotlarga kirishiga ruxsat berilmagan shaxslarning kirishini cheklash;

ushbu yo‘riqnoma da ko‘rsatilgan konfidensial ma'lumotlarning himoya qilinishini ta'minlash bo‘yicha talablar va qoidalarga rioya qilish;

konfidensial ma'lumotlar bilan ishlashda bank tomonidan belgilangan ko‘rsatmalarga rioya qilish;

konfidensial ma'lumotlar oshkor qilinganlik faktlari to‘g‘risida, shu jumladan o‘z aybi bilan oshkor qilinganlik faktlari to‘g‘risida bankning Xavfsizlik va axborotlarni muhofaza qilish departamentiga va MBXO axborotni himoya qilish bo’limiga xabardor qilishi.

146. Konfidensial ma'lumotlar bank xodimi tomonidan bank rahbariyatining roziligisiz oshkor etilishi mumkin, agar xodim ushbu konfidensial ma'lumotlarni O‘zbekiston Respublikasi qonun hujjatlariga muvofiq davlat organlariga topshirishi shart bo‘lsa. Bunda xodim konfidensial ma'lumotlarning davlat organining qonuniy talabiga ko‘ra oshkor etilishi zarur bo‘lgan qisminigina O‘zbekiston Respublikasi qonunchiligida ruxsat etilgan darajada oshkor etish majburiyatini oladi. Bunda bank xodimi bunday so‘rovlar va konfidensial ma'lumotlarni O‘zbekiston Respublikasi qonunchiligi talablariga muvofiq ushbu organlarga taqdim etish zarurligi to‘g‘risida bank rahbariyatini zudlik bilan xabardor qilish majburiyatini oladi.

147. Bank xodimi mehnat shartnomasi bekor qilingandan so‘ng moddiy tashuvchidagi konfidensial ma'lumotlarni, shuningdek ularning nusxalarini bankning birinchi so‘rovi olingan paytdan e'tiboran bir kun ichida qaytarishga yoki bank rahbariyatining ixtiyori bilan, moddiy tashuvchini (nusxalarni) yo‘q qilishga majburdir.

148. Bank rahbariyati quyidagilarni o‘z zimmasiga oladi:

bank konfidensial ma'lumotlari ro‘yxatini va bank konfidensial ma'lumotlarga yo‘l qo‘yilgan xodimlar ro‘yxatini xodimlar e'tiboriga yetkazish;

bank xodimlarini ushbu yo‘riqnoma bilan tanishtirish;

aybdor shaxslarni aniqlash uchun konfidensial ma'lumotlarni oshkor qilishning aniqlangan faktlari bo‘yicha tekshiruv o‘tkazish;

bank xodimini uning aybi bilan konfidensial ma'lumotlarni oshkor qilganligi uchun javobgarlikka tortish.

XVIII. Javobgarlik

149. Bank xodimlari tomonidan konfidensial ma'lumotlarni ruxsatsiz yig‘ish yoki elektron vositalar orqali ruxsatsiz uzatish, bunday ma'lumotlarni o‘z ichiga olgan hujjatlarni xodimlar tomonidan oshkor qilish yoki yo'qotish, konfidensial ma'lumotlarni olish yoki qasddan yo‘q qilish maqsadida serverlar va ma'lumotlar bazalariga buzib kirishi, O‘zbekiston Respublikasining amaldagi qonunchiligiga muvofiq tegishli tartibda intizomiy, ma'muriy yoki jinoiy javobgarlikka sabab bo‘ladi.

150. Konfidensial ma'lumotlar oshkor qilingan taqdirda, bank xodimi tomonidan oshkor etilishi natijasida O‘zbekiston Respublikasi qonun hujjatlariga muvofiq, Bankka yetkazilgan zararni to‘liq qoplashi shart.

151. Konfidensial ma'lumotlar chiqib ketgan yoki yoqolgan taqdirda, sizib chiqish yo‘ki yoqotish fakti bo‘yicha ichki tekshiruv o‘tkaziladi. Konfidensial

ma'lumotlarni sizib chiqishi yoki yoqolishida aybdor shaxslarni javobgarlikka tortish to‘g‘risida qaror qabul qilish uchun ichki tekshirish natijalari bank rahbariyatiga yetkaziladi.

152. Bankning konfidensial ma'lumotlarini oshkor etmaslik to‘g‘risidagi ushbu yo‘riqnomaning talablarini qasddan bajarmaslik mehnat majburiyatlarini buzish hisoblanadi va mehnat shartnomasini bekor qilishga olib keladi.

153. Mehnat shartnomasining bekor qilinishi, qanday asoslar bo‘lishidan qat'iy nazar, xodimni bankning konfidensial ma'lumotini tashkil etuvchi ma'lumotlarni oshkor etmaslik majburiyatlaridan ozod etmaydi.

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
17-ilova

Favqulodda (avariya) vaziyatlarda ish faoliyatini tiklash va uzluksiz ishlashni ta’minlash rejasi

I. Umumiy qoidalar

1. Ushbu reja “O'zsanoatqurilishbank” ATB (keyingi o‘rinlarda - bank) foydalaniladigan axborotni qayta ishlash, uzatish, saqlash texnik vositalarining uzluksiz ishlashini ta’minlashga va qisqa muddatda tiklanishiga mo‘ljallangan.

2. Bank axborot resurslari va tizimlarining uzluksiz ishlashini ta’minlash bo’yicha chora-tadbirlarga quyidagilar kiradi:

rejalashtirilgan profilaktika va ta’mirlash ishlari;

zaxira apparat vositasi;

dasturlar va ma’lumotlarning zaxira nusxasini yaratish;

uzluksiz aloqani va elektr ta’minotini ta’minlash;

server va telekommunikatsiya uskunalarining normal ishlashi uchun sharoit yaratish;

3. Bankning axborot resurslari va tizimlari faoliyatini tiklash bo’yicha chora-tadbirlarga quyidagilar kiradi:

aloqa kanallari va zaxira uskunalarini faollashtirish;

dasturlarni va ma’lumotlarni zaxira nusxalaridan tiklash;

aloqani tiklash, oqibatlarni bartaraf etish;

uskunani ta’mirlash yoki almashtirish;

dasturiy ta’minotni qayta o’rnatish.

II. Uzluksiz ishlashni ta’minlash choralari

4. Asosiy texnik vositalar: Bank domen kontrolleri serverlari, axborot tizimlari serverlari va ma’lumotlarni saqlash tizimlari, tarmoq kommutatsiya uskunalari, axborot xavfsizligi vositalarining ishlashini ta’minlash va to‘g‘ri ishlashini baholash bo‘yicha rejalashtirilgan profilaktika ishlari olib boriladi.

5. Rejali profilaktika ishlari Axborot texnologiyalari departamenti va Xavfsizlik va axborotlarni muhofaza qilish departamenti mutaxassislari tomonidan amalga oshiriladi, ularning vazifalariga 4-bandda ko'rsatilgan texnik vositalarga texnik xizmat ko'rsatish kiradi (keyingi o'rinlarda administratorlar).

6. Rejalashtirilgan profilaktika ishlari oyiga kamida bir marta quyidagi texnik vositalarga nisbatan o‘tkazilishi kerak:

lokal va korporativ tarmoq uchun telekommunikatsiya uskunalari;

axborot resurslari va tizimlarining, shu jumladan ularga o‘rnatilgan operatsion tizimlarning, MBBT va amaliy dasturlarning server uskunalari;

ma’lumotlarni saqlash tizimlari va elektron arxivlarni saqlash;

ma’lumotlarni himoyalash vositalari.

7. Rejalashtirilgan profilaktika ishlari texnik vositalarga texnik xizmat ko‘rsatish qoidalariga muvofiq amalga oshiriladi.

Profilaktik ishlar quyidagilarni o‘z ichiga oladi:

sozlamalarning yaxlitligini tekshirish;

tizim fayllarini tahlil qilish;

MBBT monitoringi;

tizimning holati, ishlashi, xatolar yuzaga kelganligi to‘g‘risidagi hisobotni (log) tekshirish;

texnik jihozlarning asosiy elementlarining ishlashini tekshirish;

diagnostika asboblaridan foydalangan holda kompleks monitoring.

8. Tuzatish ishlari administratorlar tomonidan nuqsonli apparat ishlamay qolganda yoki vositalarning ishlashini tiklash maqsadida amalga oshiriladi.

9. Profilaktik va ta’mirlash ishlarini olib borishda ish stansiyalari va serverlarini ochish va muhrlash, profilaktika ishlarini bajarish, dasturlarni o’rnatish va o’zgartirish to’g’risidagi ma’lumotlar muvofiq jurnalga qayd etiladi.

10. Administratorlar o‘zlari xizmat ko‘rsatadigan texnik vositalarning ishlashini ta’minlash uchun javobgardir.

11. Bank ishining uzluksizligini ta’minlaydigan barcha asosiy axborot tizimlari va manbalari zaxiralangan bo‘lishi kerak.

Bunday axborot tizimlari va manbalariga quyidagilar kiradi:

1) ABT - asosiy ma'lumotlarni qayta ishlash markazida klasterda (issiq zaxiralash) ishlaydigan ikkita jismoniy ma'lumotlar bazasi serverlarini tashkil qilish, shuningdek, bitta zaxira serverni tashkil qilish (ma'lumotlarning asosiy ma'lumotlar bazasidan kutish serveriga doimiy takrorlanishi) uchun taqdim etilishi kerak. - alohida jismoniy serverda sovuq kutish), shuningdek, asosiy ma'lumotlarni qayta ishlash markazidagi bir nechta virtual dastur serverlari, ular o'rtasida yuk taqsimlangan holda bank xodimlariga ABT ga kirishni ta'minlaydi, virtual dastur serverlari alohida jismoniy serverga zaxira qilinadi zaxira ma'lumotlarni qayta ishlash markazi ("sovuq zaxiralash").;

2) to'rtinchi xavfsizlik klassi IS4 (Internet-banking va mobil banking, CRM, SWIFT, Way4) va uchinchi xavfsizlik klassi IS3 (DWH, CROBS, SAP) axborot tizimlari - alohida jismoniy yoki virtual serverlarda ma'lumotlar bazasi serverining zaxira nusxasini va ilovasini tashkil etish. ularni asosiy serverdan chiqishda ("sovuq zaxira") kiritish bilan;

3) Bank domen kontrolleri– asosiy server bilan birgalikda ishlashni ta’minlovchi alohida jismoniy serverda zaxira serverini tashkil etish (“issiq-zaxirlash”);

4) Bank ERI kalitlarini ro‘yxatga olish markazi – asosiy ma’lumotlarni qayta ishlash markazida asosiy server va zaxira ma’lumotlarni qayta ishlash markazida alohida jismoniy serverda zaxira serverni tashkil etish, asosiy server chiqib ketganda zaxira serverini faollashtirish “sovuq zaxira rejimi”

Ko'rsatilgan axborot tizimlari va resurslari serverlarining zaxira bo'lishi ularga xizmat ko'rsatuvchi administratorlar tomonidan ta'minlanishi kerak.

Zaxira serverlar bankning zaxira ma’lumotlarni qayta ishlash markaziga joylashtirilishi kerak.

12. Axborot tizimlari serverlaridan tashqari bankning quyidagi texnik vositalari zaxira qilinishi mumkin:

bank korporativ tarmog‘ining asosiy kommutatorlari;

bank korporativ tarmog‘iga asosiy ma’lumotlarni qayta ishlash markazini, shuningdek, Bosh ofis (AB) va zaxira ma’lumotlarni qayta ishlash markazini ulash uchun foydalaniladigan marshrutizatorlar;

bank korporativ tarmog‘ini tashqi Internet tarmog‘iga va Markaziy bankning bank telekommunikatsiya tarmog‘iga (keyingi o‘rinlarda BTT deb yuritiladi) ulash chegarasida, shuningdek asosiy tarmoqlarni ulash chegarasida foydalaniladigan tarmoqlararo ekran va xavfsizlik shlyuzlari. ma’lumotlar markazi, shuningdek, Bosh ofis (AB) va bank korporativ tarmog‘iga zaxira ma’lumotlarni qayta ishlash markazi.

13. Axborot tizimlari va resurslarining dasturiy ta’minot va ma’lumotlarini zaxiralash bank axborot xavfsizligi siyosatiga 6-ilovada keltirilgan Tizim va amaliy dasturiy ta’minotni yangilash, shuningdek ma’lumotlarni zaxiralash va tiklash to‘g‘risidagi nizomga muvofiq amalga oshiriladi.

14. Uzluksiz elektr ta'minoti va aloqani ta'minlash uchun quyidagi choralar ko'rilishi kerak:

bank bosh ofis (ab va zaxira ma’lumotlarni qayta ishlash markazi) va asosiy ma’lumotlarni qayta ishlash markazi binosiga dizel generatorlarini o‘rnatish;

bank asosiy va zaxira ma’lumotlarni qayta ishlash markazlarida jihozlarni uzluksiz elektr energiyasi bilan ta’minlash uchun uzluksiz quvvat manbalaridan foydalanish;

server va tarmoq uskunalarini uzluksiz quvvat bilan ta'minlash uchun uzluksiz quvvat manbalaridan foydalanish, asosiy va zaxira ma'lumotlarni qayta ishlash markazlarining server xonasida (server raflari), shuningdek, bankning MBXO va BXM server xonalarida joylashgan axborotni himoya qilish vositalari.

15. Bank binosining kafolatlangan elektr ta’minoti tizimida asosiy ma’lumotlarni qayta ishlash markazi binosi va bank Bosh ofis binosi (AB va zaxira ma’lumotlarni qayta ishlash markazi) uchun turli stansiyalardan ikkita quvvat manbai bo‘lishi kerak.

16. Elektr uzatish liniyalari, avtomatik dizel elektr stansiyasining parametrlari va uning zaxirasi bank uskunalari va tizimlari tomonidan iste’mol qilinadigan umumiy quvvatdan kelib chiqqan holda belgilanadi va energiya zaxirasining kamida 10 foizini tashkil qilishi kerak.

Dizel elektr stansiyalari uzluksiz ishlashi uchun kamida bir kunlik yoqilg'i ta'minoti bo'lishi va elektr yo'qligida avtomatik ravishda ishga tushishi kerak.

17. Bank korporativ tarmog‘ini tashqi Internet tarmog‘iga va Markaziy bankning BTTiga ulash uchun, shuningdek, MBXO va BXMni korporativ tarmoqdagi asosiy ma’lumotlarni qayta ishlash markaziga ulashda foydalaniladigan aloqa kanallari zaxiraga olinadi.

18. Bankning asosiy telekommunikatsiya uskunalari, ma’lumotlar bazalari, axborot tizimlari serverlari va axborot xavfsizligini ta’minlash vositalari asosiy va zaxira ma’lumotlarni qayta ishlash markazlarining server xonalarida joylashtirilishi kerak.

19. Server xonalari asosiy va zaxira ma’lumotlarni qayta ishlash markazi kombinatsiyalangan qulflar, (biometrik yoki boshqa usullar) videokuzatuv tizimi, uzluksiz quvvat manbalari bilan ta’minlanishi, binoning yong‘inga qarshi tizimiga ulanmagan avtomatik gazli o‘chirish tizimi bilan jihozlangan, shuningdek O’z DSt 2875: 2014 Davlat standarti talablariga hamda Markaziy banki Boshqaruvining 2020 yil

25 yanvardagi 2/4-sonli "O'zbekiston Respublikasi tijorat Banklarining avtomatlashtirilgan tizimlarida axborotni muhofaza qilish to'g'risidagi nizomni tasdiqlash to'g'risida" gi qaroriga muvofiq iqlim sharoitlari bilan ta'minlangan bo'lishi kerak.

III. Qayta tiklash choralari

20. Avariya yoki favqulodda vaziyatlarda axborot tizimlari va resurslarining holatini tiklash jadvalda keltirilgan tasdiqlangan favqulodda vaziyatlarni tiklash rejasiga muvofiq amalga oshirilishi kerak.

21. Har bir axborot tizimi va o'ta muhim himoya obyektlari (domen boshqaruvchisi serverlari, axborot almashish tizimlari, asosiy kommutatorlar va marshrutizatorlar, axborotni himoya qilish vositalari) uchun favqulodda vaziyatlarni tiklashning batafsil rejasi bo'lishi kerak. Axborot tizimlari va muhim himoya qilish obyektlarini qayta tiklash Axborot texnologiyalari departamenti hamda Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimlari tomonidan batafsil tiklash rejalariga muvofiq amalga oshirilishi kerak. Qayta tiklash rejalari jalb qilingan xodimlarning xatti-harakatlarini va xodimlarning favqulodda vaziyatlar va favqulodda vaziyatlarga tayyorgarligini qamrab olishi kerak.

22. Baxtsiz hodisa sodir bo'lgan taqdirda axborot tizimlari va resurslarining ishlashini tiklash bo'yicha chora-tadbirlar zaxira texnik vositalar yoki resurslarni kiritish, eskirgan texnik vositalarni almashtirish, dasturiy ta'minotni tiklash yoki qayta o'rnatish, zaxira media arxiv nusxalaridan ma'lumotlarni tiklash yoki qayta tiklashni o'z ichiga oladi..

23. Tasdiqlangan tiklanish rejalariga muvofiq, o'quv mashg'ulotlari yiliga kamida ikki marta o'tkazilishi kerak. Trening davomida barcha bajarilgan ishlar hujjatlashtirilishi kerak.

O'quv jarayonida aniqlangan kamchiliklar xodimlar tomonidan tiklanish harakatlarini qayta bajarish orqali tuzatilishi kerak. Trening natijalariga ko'ra, batafsil tiklanish rejalariga o'zgartirishlar kiritilishi mumkin.

24. Axborot tizimlari va resurslarining holatini tiklash uchun ma'lumotlarni qayta tiklash tizimlarini jalb qilish kerak. Axborot texnologiyalari departamenti xodimlari har oyda kamida bir marta ma'lumotlarni qayta tiklash tizimlarining holatini tekshirib turishlari va tekshirish natijalarini maxsus kitobga yozib borishlari shart. Agar kamchiliklar aniqlansa, aniqlangan kamchiliklar, ushbu kamchiliklarni bartaraf etish choralari va muddatlari ko'rsatilgan dalolatnoma tuzilishi kerak.

25. Har bir axborot tizimi uchun batafsil tiklash rejalari quyidagi favqulodda vaziyatlarni va bosqichma-bosqich harakatlarni belgilashi kerak:

1) Elektr uzilishi:

Bosqichma-bosqich choralar:

markaziy apparat va filiallarning server xonasida joylashgan server uskunalari uchun zaxira quvvat manbai UPS (ularning avtomatik ishlashi ta'minlangan) avtomatik ravishda yoqilganligini va ishlashini tekshirish;

serverlar va tarmoq uskunalarining ishlashini tekshirish;

tashqi elektr ta'minotini tiklash uchun sabablar va zarur vaqtni aniqlash uchun RESga qo'ng'iroq qilish, kerak bo'lganda elektrchini chaqirish;

asosiy elektr ta’minotini tiklash, zaxira quvvat manbalarini zaryadlash;

2) Aloqa yo'qolishi (tarmoq kabellari, korporativ tarmoq ma'lumotlar havolalari, tashqi tarmoq ulanishlari va tashqi axborot tizimlari bilan integratsiya uchun foydalaniladigan havolalar):

Bosqichma-bosqich choralar:

yo’qolgan ulanishning barcha sohalarida kanallarni tekshirish va tarmoq uskunalari - marshrutizatorlar, kalitlar, tarmoq kabelining holati;

nosozlik sababini aniqlash;

zaxira tarmoq uskunasidan foydalangan holda aloqani tiklash yoki tarmoq kabelini almashtirish;

ma’lumotlarni uzatish tarmog’i operatorlaridan biri bilan tashqi aloqa uzilgan taqdirda trafikni alohida aloqa liniyasiga o’tkazish;

Internet tarmog’iga ulanganda tashqi aloqa yo’qolgan taqdirda ma’lumotlarni uzatish tarmog’i operatori bilan aloqa qilish;

muvaffaqiyatsiz tashqi aloqani tiklash;

ishlamay qolgan tarmoq uskunalarini ta’mirlash.

3) Serverlarning ishlamay qolishi:

zaxira serverining ishlashini va axborot xavfsizligini nazorat qilish (issiq kutish rejimidan foydalanadigan axborot tizimlari uchun);

sovuq zaxira tizimlari uchun kutish serverida ma'lumotlarni yig'ish va zaxira serverini ishga tushirish;

ishlamay qolgan serverning ishlamay qolishi sabablarini aniqlash - server va uning komponentlari, operatsion tizim, MBBT va amaliy dasturlar (diagnostika vositalari) ishini tekshirish;

muammolarni bartaraf yetish - server komponentini almashtirish, operatsion tizimni tasvirdan tiklash, dasturni qayta ishga tushirish yoki qayta o’rnatish va h.k;

qayta tiklangan serverning to’g’ri ishlashini tekshirish va uni ishga tushirish.

Yuqoridagi harakatlar choralari 1-jadvalda ko'rsatilgan mas'ul xodimlar tomonidan amalga oshirilishi kerak.

26. Qayta tiklash ishlarini olib borishda va hodisa oqibatlarini bartaraf etishda quyidagi hujjatlarga rioya qilish kerak:

axborot tizimini tiklash bo’yicha batafsil reja;

zaxira nusxasini yaratish va ma’lumotlarni tiklash qo’llanmasi;

ma’lumotlarni saqlash tizimi, aloqa vositalari va axborotni muhofaza qilish bo’yicha foydalanish ko’rsatmalari;

bino ichidagi tarmoq topologiyasi;

dizel generatorini elektr bilan ta’minlash va ulash sxemasi;

favqulodda vaziyatlarda evakuatsiya qilish rejasi;

ma’lumotlar uzatish tarmog’i operatori bilan tuzilgan xizmat ko’rsatish shartnomasi;

O’zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi hamda davlat va xo’jalik boshqaruvi organlari o’rtasida axborot xavfsizligi hodisalariga javob berish, tergov va oldini olish bo’yicha o’zaro hamkorlik reglamenti.

IV. Favqulodda vaziyatlar yuzasidan choralar

27. Tabiiy va texnogen hodisalar natijasida yuzaga kelgan favqulodda vaziyatlarda bank axborot tizimlarining ishlashini ta’minlash uchun zaxira ma’lumotlarni qayta ishlash markazi resurslaridan foydalanish kerak.

Zaxira ma'lumotlarni qayta ishlash markazi asosiy ma'lumotlarni qayta ishlash markaziga qo'llaniladigan barcha talablarga javob berishi kerak.

28. Ushbu chora-tadbirlar 11-bandda ko'rsatilgan axborot tizimlari va 12-bandda ko'rsatilgan texnik vositalar uchun taqdim etilishi kerak.

29. Zaxira ma'lumotlarni qayta ishlash markazi korporativ tarmoqqa, tashqi Internet tarmog'iga va Markaziy bankning BTTga doimiy ulanishiga ega bo'lishi kerak.

30. Zaxira ma'lumotlarni qayta ishlash markazidan to'liq foydalanish uchun quyidagilar amalga oshiriladi:

korporativ tarmoq va tashqi tarmoqning tarmoq trafigini faqat zaxiraviy ma'lumotlarni qayta ishlash markaziga o'tkazish (asosiy ma'lumotlarni qayta ishlash markazi qayta tiklanmaguncha);

issiq kutish rejimida ishlaydigan ma'lumotlar bazasi serverlari, ilovalari va ma'lumotlarni saqlash tizimlarining ishlashi va ma'lumotlarining to'liqligini tekshirish;

zarur hollarda zaxira ma'lumotlarni qayta ishlash markazining bepul resurslaridan foydalanish;

sovuq zaxiradagi serverlarni ishga tushirish;

bank administratorlari tomonidan ma’lumotlar markazining zaxiraviy ma’lumotlarini qayta ishlash, saqlash, uzatish va himoya qilish vositalari ustidan to‘liq nazoratni olish va ularning faoliyati ustidan doimiy monitoring olib borish.

31. Axborot tizimlarining ishlashini tiklash uchun ma'lumotlarni qayta ishlash markazining zaxiraviy nusxasidan foydalanishning iloji bo'lmasa, zaxira rejasi taqdim etilishi kerak: respublika hududida ma'lumotlarni qayta ishlash markazi faoliyat yurituvchi boshqa operatorlarning bepul resurslaridan foydalanish.

V. Hodisalar va favqulodda vaziyatlarni boshqarish, shuningdek, uchinchi tomon tashkilotlari bilan o’zaro aloqalar bo’yicha reglament

32. Bankda baxtsiz hodisalar va favqulodda vaziyatlar axborot xavfsizligi hodisalari sifatida ko‘rib chiqilishi va ular bank Axborot xavfsizligi siyosatiga 18-ilovada keltirilgan Axborot xavfsizligi hodisalariga javob choralari ko‘rish nizomiga muvofiq boshqarilishi lozim.

33. Har bir baxtsiz hodisa va favqulodda vaziyat uchun qo'shimcha choralar ko'rish kerak:

avariya va favqulodda vaziyat haqida Xavfsizlik va axborotni muhofaza qilish departamentiga xabar berish;

bank Axborot xavfsizligi siyosatiga 18-ilovada keltirilgan bankning Favqulodda xavfsizlik holatlari jurnalida yuzaga kelgan vaziyatni aniqlash;

restavratsiya rejalariga muvofiq restavratsiya ishlarini amalga oshirish.

34. Bankning tarkibiy bo'linmalari xodimlari va rahbarlari har bir baxtsiz hodisa va favqulodda holat to'g'risida zudlik bilan Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga hisobot berishga majburdirlar.

35. Bankda avariya va favqulodda vaziyatlar sodir bo‘lgan taqdirda, O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi va davlat va xo‘jalik boshqaruvi organlari axborot xavfsizligi hodisalariga javob berish, tekshirish va oldini olish uchun o‘rtasidagi o‘zaro hamkorlik to‘g‘risidagi nizomga muvofiq “Kiberxavfsizlik markazi” DUK bilan o‘zaro hamkorlik qilishi shart.

1-Jadval

Favqulodda (avariya) vaziyatlarda ish faoliyatini tiklash va uzluksiz ishlashni ta’minlash Rejasi

Avariya yoki nosozlik nomi	Harakatlar bosqichlari	Bajarilish vaqti *	Mas’ullar
Avariya vaziyatlari			
1. Elektr ta’minotining uzilishi (to‘liq yoki qisman)			
Bosh ofis (zaxira ma’lumotlarni qayta ishlash markazi) va asosiy ma’lumotlarni qayta ishlash markazining elektr quvvati uzilishi	1) Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar berish; 2) sabablarini va zarur tiklanish vaqtini aniqlash uchun RESga qo’ng’iroq qilish, agar kerak bo’lsa, elektrchini chaqirish, 3) serverlar, tarmoq uskunalari va himoya uskunalari uchun zaxira quvvat manbaining avtomatik ravishda yoqilishi va ishlashini tekshirish; 4) binoda dizel generatorini avtomatik ravishda yoqishni tekshirish; 5) muqobil quvvat manbaidan foydalanish jarayonida asosiy serverlar, tarmoq uskunalari va himoya vositalarining ishlashini tekshirish va monitoring qilish; 6) asosiy elektr ta’minotini tiklash, zaxira quvvat manbalarini zaryadlash.	1-5 daqiqa 1-5 daqiqa 1-5 daqiqa 1-5 daqiqa 1 va undan ko’proq daqiqa 1 va undan ko’proq soat	Axborot texnologiyalari departamenti, Xavfsizlik va axborotlarni muhofaza qilish departamenti
MBXO va BXMda elektr uzilishi	1) Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar berish; 2) sabablarini va zarur tiklanish vaqtini aniqlash uchun RESga qo’ng’iroq qilish, agar kerak bo’lsa, elektrchini chaqirish, 3) serverlar, tarmoq uskunalari va himoya uskunalari uchun zaxira quvvat manbaining avtomatik ravishda yoqilishi va ishlashini tekshirish; 4) binoda dizel generatorini avtomatik ravishda yoqishni tekshirish; 5) muqobil quvvat manbaidan foydalanish jarayonida asosiy serverlar, tarmoq uskunalari va himoya vositalarining ishlashini tekshirish va monitoring qilish; 6) asosiy elektr ta’minotini tiklash, zaxira quvvat manbalarini zaryadlash.	1-5 daqiqa 5-10 daqiqa 1-5 daqiqa 1-5 daqiqa 1 va undan ko’proq daqiqa 1 va undan ko’proq soat	MBXOning Axborot texnologiyalari bo’limlari va Xavfsizlik va axborotni muhofaza qilish bo’limlari
2. Aloqa uzilishi			

Tashqi aloqaga zarar yetkazish – korporativ tarmoqni tashqi Internet tarmog‘iga va Markaziy bankning bank telekommunikatsiya tarmog‘iga ulash.	1) Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar berish; 2) tashqi ulanish kanallarini (telekommunikatsiya operatoriga aloqaga chiqish), tarmoq uskunasining ishlashini – tarmoqlararo ekran, kommutatorlar, tarmoq kabelining holatini tekshirish (nosozlik sabablarini aniqlash); 3) tashqi tarmoqqa zaxiraviy ulanishni faollashtirish; 4) trafikni ishlaydigan tashqi aloqa kanallariga o’tkazish (marshrutlash jadvalini o’zgartirish); 5) aloqani tiklash jarayonini kuzatish uchun uning tarmog’ida aloqa uzilgan taqdirda aloqa operatori bilan doimiy aloqada bo’lish; 6) ishlamay qolgan uskunani ta’mirlash yoki yangisini sotib olish, eski marshrutlash sozlamalarini qaytarish, aloqani to’liq tiklash.	1-10 daqiqa 5-20 daqiqa 10-20 daqiqa 10-20 daqiqa Aloqa yoqolganda Qayta ulanishdan keyin	Axborot texnologiyalari departamenti, Xavfsizlik va axborotlarni muhofaza qilish departamenti, Korporativ tarmoq administratori
Bosh ofisning korporativ tarmog'iga (AB va zaxira ma'lumotlarni qayta ishlash markazi) va asosiy ma'lumotlarni qayta ishlash markaziga ulanishning shikastlanishi	1) Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar berish; 2) tashqi ulanish kanallarini (telekommunikatsiya operatoriga aloqaga chiqish), tarmoq uskunasining ishlashini – tarmoqlararo ekran, kommutatorlar, tarmoq kabelining holatini tekshirish (nosozlik sabablarini aniqlash); 3) tashqi tarmoqqa zaxiraviy ulanishni faollashtirish; 4) trafikni ishlaydigan tashqi aloqa kanallariga o’tkazish (marshrutlash jadvalini o’zgartirish); 5) aloqani tiklash jarayonini kuzatish uchun uning tarmog’ida aloqa uzilgan taqdirda aloqa operatori bilan doimiy aloqada bo’lish; 6) ishlamay qolgan uskunani ta’mirlash yoki yangisini sotib olish, eski marshrutlash sozlamalarini qaytarish, aloqani to’liq tiklash.	1-10 daqiqa 5-20 daqiqa 10-20 daqiqa 10-20 daqiqa Aloqa yoqolganda Qayta ulanishdan keyin	Axborot texnologiyalari departamenti, Xavfsizlik va axborotlarni muhofaza qilish departamenti, Korporativ tarmoq administratori

MBXO, BXM, masofaviy kassalarning korporativ tarmoqqa ulanishiga zarar yetkazish	1) Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar berish; 2) Korporativ tarmoq administratoriga xabar berish; 3) aloqa kanallarini tekshirish, tarmoq uskunalari – marshrutizatorlar, modemlar, kommutatorlar, tarmoq kabelining holati (nosozlik sabablarini aniqlash); 4) tarmoq ichidagi nosozliklar yuzaga kelganda, zaxira tarmoq uskunasidan foydalangan holda aloqani tiklash yoki tarmoq kabelini almashtirish; 5) asosiy ma'lumotlarni qayta ishlash markazi va MBXO, BXM o'rtasidagi trafikni ishlaydigan korporativ aloqa kanallariga o'tkazish (marshrutlash jadvalini o'zgartirish); 6) aloqani tiklash jarayonini kuzatish uchun uning tarmog'ida aloqa uzilgan taqdirda aloqa operatori bilan doimiy aloqada bo'lish; 7) ishlamay qolgan uskunani ta'mirlash yoki yangisini sotib olish, eski marshrutlash sozlamalarini qaytarish, aloqani to'liq tiklash.	5-10 daqiqa 5-10 daqiqa 10-20 daqiqa 20-30 daqiqa 20-30 daqiqa Aloqa yoqolganda Qayta ulanishdan keyin	Axborot texnologiyalari departamenti, Xavfsizlik va axborotlarni muhofaza qilish departamenti, Korporativ tarmoq administratori, MBXOning Axborot texnologiyalari bo'limlari, Korporativ tarmoq administratori
3. Axborot tizimlari va serverlarning ishdan chiqishi			
Ilova serverlari va ma'lumotlar bazasining ishlamay qolishi (serverning jismoniy komponentining ishlamay qolishi – protsessor, operativ xotira, ona palata, tarmoq kartasi va boshqalar).	1) Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar berish; 2) zaxira serverini ishga tushirish va/yoki boshqarish va axborot xavfsizligini ta'minlash (issiq zaxira rejimidan foydalanadigan axborot tizimlari uchun); 3) sovuq zaxira tizimlari uchun zaxira serverida ma'lumotlarni kompilyatsiya qilish va qayta tiklangan yoki zaxiralangan ma'lumotlar bilan zaxira serverni ishga tushirish; 4) ishlamay qolgan serverning ishdan chiqishi sabablarini aniqlash; 5) muvaffaqiyatsiz serverni ta'mirlash yoki muvaffaqiyatsiz komponentni almashtirish; 6) muvaffaqiyatsiz serverni tiklash; 7) asosiy serverdagi ma'lumotlarni qayta tiklash (agar yagona saqlash tizimi ishlatilmasa) va serverni ishga tushirish.	5-10 daqiqa 5-10 daqiqa 10-30 daqiqa 10-30 daqiqa 1 soatdan 2 sutkagacha 1 soatdan 2 sutkagacha 1 soatdan 2 sutkagacha	Axborot texnologiyalari departamenti, server administratori

Tizim yoki amaliy dasturiy ta’minotning ishlamay qolishi	1) Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar berish; 2) zaxira serverining ishlashini va ma’lumotlarning xavfsizligini nazorat qilish (issiq zaxira rejimidan foydalanadigan axborot tizimlari uchun); 3) sovuq zaxira tizimlari uchun zaxira serverida ma’lumotlarni kompilyatsiya qilish va qayta tiklangan yoki zaxiralangan ma’lumotlar bilan zaxira serverni ishga tushirish; 4) ishlamay qolgan serverning ishdan chiqishi sabablarini aniqlash; 5) tizim dasturini tasvirdan tiklash yoki muvaffaqiyatsiz serverda amaliy dasturni qayta o’rnatish; 6) muvaffaqiyatsiz serverni tiklash; 7) asosiy serverdagi ma’lumotlarni qayta tiklash (agar yagona saqlash tizimi ishlatilmasa) va serverni ishga tushirish.	5-10 daqiqa 5-10 daqiqa 10-30 daqiqa 10-30 daqiqa 1-2 soat 1-2 soat 1-2 soat	Axborot texnologiyalari departamenti, axborot tizimi administratori
4. Tabiiy va texnogen hodisalar natijasida yuzaga kelgan favqulodda vaziyatlar			
bank axborot tizimlarining ishlashini ta’minlash	1) Axborot texnologiyalari departamenti direktoriga va Xavfsizlik va axborotlarni muhofaza qilish departamenti direktoriga xabar berish; Zaxira ma'lumotlarni qayta ishlash markazini faollashtirish: 2) korporativ va tashqi tarmoqlarning tarmoq trafigini faqat zaxiraviy ma'lumotlarni qayta ishlash markaziga o'tkazish (asosiy ma'lumotlarni qayta ishlash markazi tiklanmaguncha) - zaxiraviy ma'lumotlarni qayta ishlash markazida zaxira yadro kommutator va tarmoqlararo ekrandan foydalanish; 3) zaxiraviy ma'lumotlarni qayta ishlash markazida axborot tizimlari va resurslarining zaxira serverlarini faollashtirish va ma’lumotlar bazasi serverlari, ilovalari va ma’lumotlar bazasining zaxiraviy ma’lumotlarini saqlash tizimi ma’lumotlarining to‘liqligini tekshirish; 4) administratorlar tomonidan zaxiraviy ma'lumotlarini qayta ishlash markazining, ma'lumotlar saqlash va uzatish vositalarini to'liq nazorat qilish va ularning ishlashi ustidan doimiy monitoringni ta'minlash.	5-10 daqiqa 20-30 daqiqa 4-6 soat 1 soat - 1 sutka	Axborot texnologiyalari departamenti, server administratori, axborot tizimi administratori

Izox:

1) "Ish vaqti" ustunida avariya sodir bo‘lgan va aniqlangan vaqtdan boshlab vaqt ko‘rsatiladi;

Favqulodda (avariya) vaziyatlarda ish faoliyatini tiklash va uzluksiz ishlashni ta’minlash Rejasiga ilova

Ish stansiyalari va serverlarni ochish va muhrlash, profilaktika ishlarini bajarish, dasturlarni o‘rnatish va o‘zgartirishlarni qayd etish jurnali

№	Sana	Hodisa	Javobgar imzosi

“O‘zsanoatqurilishbank”
ATBning axborot xavfsizligi
siyosatiga 18-ilova

Axborot xavfsizligi hodisalariga javob berish qoidalari

I. Umumiy qoidalar

1. “O‘zsanoatqurilishbank” ATBning axborot xavfsizligi hodisalariga javob berish Qoidalari (keyingi o‘rinlarda – Qoidalar) quyidagilarni belgilaydi:

bank axborot xavfsizligi hodisalarini boshqarish tartib-taomillarini amalga oshirish tartibi;

tarkibiy bo‘linmalari va mutaxassislarining axborot xavfsizligi hodisalarini boshqarish tartib-taomillarini amalga oshirishda o‘zaro hamkorligi tartibi;

bankning axborot xavfsizligi hodisalarini boshqarishda tashqi tashkilotlar bilan o‘zaro hamkorligi tartibi;

axborot xavfsizligi hodisalarini boshqarish jarayonlarini hujjatlashtirish tartibi.

2. Axborot xavfsizligi hodisalarini boshqarish tartib-taomillarini amalga oshirishda bank tarkibiy bo‘linmalari va mutaxassislari ushbu Qoidalarga muvofiq aniq va izchil harakatlarni amalga oshirishlari hamda bir-biri bilan o‘zaro hamkorlik qilishlari shart.

3. Ushbu hujjat bank axborot xavfsizligi siyosatida belgilangan himoya qilish obyektlariga nisbatan sodir bo‘lgan barcha hodisalarga nisbatan qo‘llaniladi.

4. Ushbu Qoidalar talablari bankning Bosh ofisida va AB, MBXO, BXM, masofaviy kassalarida axborot xavfsizligi hodisalarini boshqarishda majburiydir.

5. Ushbu hujjat Bankda axborot xavfsizligi hodisalarini boshqarish bilan shug‘ullanuvchi barcha xodimlarga qo’llaniladi.

II. Atamalar, ta'riflar va qisqartmalar

6. Ushbu hujjatda quyidagi atamalar va ularning ta'riflari qo'llaniladi:

1) **axborot xavfsizligi hodisasiga javob berish:** axborot xavfsizligi hodisasini yumshatish yoki bartaraf etish bo'yicha ko'riladigan harakatlar, shu jumladan axborot tizimi va unda saqlanadigan ma'lumotlarning normal ishlash rejimlarini himoya qilish va tiklash bo'yicha ko'rilgan choralar;

2) **axborot xavfsizligi hodisasi:** tizim, xizmat yoki tarmoq holatida axborot xavfsizligi siyosatining mumkin bo‘lgan buzilishi yoki himoyalanmaganligini ko‘rsatuvchi aniqlangan hodisa yoki axborot xavfsizligi uchun ahamiyatli bo‘lishi mumkin bo‘lgan erta noma’lum holat;

3) **Axborot xavfsizligi hodisalarini boshqarish:** axborot xavfsizligi hodisalarini aniqlash, qayd etish, baholash, javob berish va tekshirish jarayonlari.

III. Axborot xavfsizligi hodisalarini boshqarish majburiyatlari

7. Bank rahbariyati hamda bank AB, MBXO, BXM rahbariyatining axborot xavfsizligi hodisalarini boshqarish bo‘yicha vazifalariga quyidagilar kiradi:

a) axborot xavfsizligi hodisalarini boshqarish protseduralari yoki jarayonlarini o'tkazishga rozilik berish yoki kelishib berish;

b) mas'uliyatni taqsimlash va axborot xavfsizligi hodisalarini boshqarish uchun mas'ul shaxslarni tayinlash;

c) hodisani bartaraf etish, uning oqibatlarini bartaraf etish va hodisalarning takrorlanishining oldini olish bo'yicha chora-tadbirlarni amalga oshirish uchun resurslarni ajratish yoki taqsimlash;

d) tashqi uchinchi tomon tashkilotlarini xabardor qilish va axborot xavfsizligi hodisalarini boshqarish jarayoniga jalb qilish bo'yicha qarorlar qabul qilish;

e) axborot xavfsizligi hodisalari bo'yicha tekshiruvlar o'tkazish bo'yicha guruh tarkibini kelishish;

f) aybdorlarga jazo tayinlash.

8. Bank xodimlarining axborot xavfsizligi hodisalarini boshqarish jarayonida quyidagi vazifalari belgilab qo‘yiladi:

a) axborot xavfsizligi talablari va qoidalariga rioya qilish;

b) aniqlangan yoki ularga ma'lum bo'lgan axborot xavfsizligi hodisalari to'g'risida darhol xabar berish;

s) agar ularga nisbatan qat'iy choralar ko'rilmasa, oqibatlarga olib kelishi mumkin bo'lgan huquqbuzarliklar faktlarini yashirishga yo'l qo'yilmasligi;

d) bank tizimlari va xizmatlarida kuzatilgan yoki shubha qilingan axborot xavfsizligi kamchiliklari haqida xabar berish;

e) bankka ko‘proq zarar yetkazishi mumkin bo‘lgan hodisalar oqibatlarini bartaraf etish bo‘yicha kelishilmagan harakatlarga yo‘l qo‘yilmasligi;

f) hodisalarni tekshirishda yordam berish.

9. Bankning quyidagi mas’ul tarkibiy bo‘linmalari va mutaxassislari axborot xavfsizligi hodisalarini boshqarish jarayonlariga jalb etilishi mumkin:

a) axborot tizimlari, tarmoqlari va boshqa axborotlashtirish obyektlarini saqlash uchun mas'ul bo'lgan Axborot texnologiyalari departamenti xodimlari;

b) Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimlari;

c) MBXOdagi Axborot texnologiyalari bo'limlari va Xavfsizlik va axborotni muhofaza qilish bo'limlari xodimlari;

d) Kadrlarni boshqarish departamenti xodimlari, axborot xavfsizligi hodisalarini boshqarishda xodimlarning xabardorligini oshirish va mas'uliyatni yuklash nuqtai nazaridan;

e) buxgalteriya hisobi va moliyaviy menejment departamenti xodimlari, zararni, yo'qotishlarni baholash nuqtai nazaridan;

f) axborot xavfsizligi buzilishi bilan bog'liq bank uchun risklarni baholash nuqtai nazaridan Risklarni boshqarish departamenti xodimlari va boshqalar.

10. Axborot xavfsizligi hodisalariga tezkor chora ko‘rish uchun Bankda doimiy faoliyat ko‘rsatuvchi Voqealarga qarshi kurash guruhi tuziladi, uning tarkibi bank buyrug‘i bilan belgilanadi.

11. Bank axborot xavfsizligi hodisalariga qarshi kurash guruhining vazifalariga quyidagilar kiradi:

a) axborot xavfsizligiga tahdidning harakatini mahalliylashtirish va zararsizlantirish bo'yicha tadbirlar va chora-tadbirlarni amalga oshirish;

b) axborot xavfsizligi hodisasi oqibatlarini baholash;

c) qayta tiklash ishlarini tashkil etish va o'tkazish va axborot xavfsizligi hodisasi oqibatlarini bartaraf etish;

d) axborot xavfsizligi hodisalarini tahlil qilish.

IV. Axborot xavfsizligi hodisalarini boshqarish bo'yicha tayyorgarlik chora-tadbirlari

12. Axborot xavfsizligi hodisalarini samarali boshqarish uchun Bankda quyidagi tayyorgarlik choralarini ko‘rish zarur:

hodisalarga javob berish uchun mas'ul xodimlar uchun hodisalarni boshqarish bo'yicha trening;

xodimlarni hodisalarni boshqarish tartib-qoidalari bilan tanishtirish;

xodimlar o'rtasida ko'nikmalarni rivojlantirish va tezkorlikni oshirish uchun hodisalarni boshqarishning belgilangan tartib-qoidalarini amalga oshirish yoki tabiiy ofatlarni tiklash rejalarini sinovdan o'tkazish bo'yicha muntazam mashg'ulotlar o'tkazish;

xodimlarni hodisalarni boshqarish bo'yicha o'z vazifalari va javobgarliklari to'g'risida xabardor qilish;

voqea sodir bo'lgan taqdirda ichki va tashqi resurslarni zaxiralash;

hodisalarni boshqarishda o'zaro hamkorlik qilish zarur bo'lgan tashqi tashkilotlar bilan aloqalarni o'rnatish;

bank tarkibiy bo‘linmalaridan sodir bo‘lgan voqealar to‘g‘risida ma’lumotlarni to‘plash, “Ishonch telefoni”ni bank tarkibiy bo‘linmalari va xodimlariga yetkazish uchun Xavfsizlik va axborotlarni muhofaza qilish departamenti uchun “ishonch telefoni”ni tashkil etish;

Xavfsizlik va axborotni muhofaza qilish departamentida axborot xavfsizligi hodisalarini monitoring qilish, axborot xavfsizligi hodisalarini to'plash, hisobga olish va ro'yxatga olish uchun mas'ul xodimlarni tayinlash.

13. Axborot xavfsizligi hodisalarini boshqarish bo'yicha tayyorgarlik chora-tadbirlarini amalga oshirish Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan Axborot texnologiyalari boshqarmasi bilan birgalikda ta'minlanadi.

14. Xavfsizlik va axborotlarni muhofaza qilish departamenti Kadrlarni boshqarish departamenti bilan birgalikda yiliga kamida bir marta davriy ravishda quyidagilarni amalga oshirishi shart:

bosh ofis va AB xodimlari o'rtasida ushbu hujjatda belgilangan hodisalarni boshqarish bo'yicha ularning vazifalari va majburiyatlari to'g'risida tushuntirish ishlarini olib borish;

hodisalarga javob berish uchun mas'ul xodimlar uchun hodisalarni boshqarish bo'yicha treninglarni tashkil etish.

MBXO va BXMda xodimlari o'rtasida axborot xavfsizligi hodisalarini boshqarish bo'yicha majburiyatlari va majburiyatlari bo'yicha tushuntirish ishlari MBXO Xavfsizlik va axborotni muhofaza qilish bo'limlari tomonidan MBXOda xodimlarni boshqarish bo'yicha tarkibiy bo'linmalar bilan birgalikda amalga oshiriladi.

15. Hodisalarni boshqarish bo'yicha treningning bir qismi sifatida hodisalarga javob berish uchun mas'ul bo'lgan xodimlar hodisalarni boshqarish bo'yicha o'zlarining vazifalari va mas'uliyatlari haqida xabardor bo'lishlari kerak.

16. Xavfsizlik va axborotlarni muhofaza qilish departamenti muntazam ravishda yiliga kamida bir marta ushbu hujjatda belgilangan hodisalarni boshqarish tartib-qoidalarini amalga oshirish va tabiiy ofatlarni tiklash rejalarini sinovdan o'tkazish bo'yicha o'quv mashg'ulotlarini tashkil qiladi va o'tkazadi.

17. Xavfsizlik va axborotlarni muhofaza qilish departamenti hodisalarni boshqarishda o'zaro aloqada bo'lishi kerak bo'lgan tashqi tashkilotlarning barcha aloqalariga ega bo'lishi kerak.

V. Axborot xavfsizligi hodisalarini boshqarish tartibi

18. Axborot xavfsizligi hodisalarini aniqlash uchun monitoring jarayoni quyidagilarni o'z ichiga olishi kerak:

1) Bank Bosh boshqarmasi, AB, MBXO, BXM, masofaviy kassalar xodimlariga quyidagi himoya obyektlariga nisbatan:

ular foydalanadigan ish stansiyalari va ularda o'rnatilgan dasturiy ta'minot;

ularga foydalanish uchun berilgan axborot tashuvchilar;

foydalanuvchilari bo'lgan axborot tizimlari;

2) Bankning konfidensial ma’lumotlarning egalari bo‘lgan tarkibiy bo‘linmalari va konfidensial ma’lumotlarga yo‘l qo‘yilgan xodimlarga quyidagi himoya obyektlariga nisbatan:

konfidensial ma'lumotlar, shu jumladan tijorat sirlari, bank sirlari, shaxsiy ma'lumotlar va "Xizmatda foydalanish uchun" belgisi bo'lgan hujjatlar;

konfidensial ma'lumotlarni qayta ishlash va konfidensial hujjatlarni qog'oz shaklida saqlash amalga oshiriladigan himoyalangan binolar;

3) Axborot texnologiyalari departamenti:

ABT va boshqa axborot tizimlari, shuningdek ularning ma'lumotlar bazasi serverlari va ilovalari, dasturiy ta'minoti;

korporativ tarmoq va uning tarmoq uskunalari, domen kontroller serverlari, shuningdek, korporativ tarmoqni tashkil qilish uchun foydalaniladigan tashqi aloqa kanallari;

bank va ABdagi lokal tarmoq, shuningdek, ularning tarmoq uskunalari, kabel tizimi tarkibiga kiruvchi bankning asosiy va zaxira ma’lumotlarni qayta ishlash markazidagi lokal tarmoq va SAN;

axborot almashish tizimlari: korporativ elektron pochta, Banklararo elektron pochta, IP-telefoniya va videokonferensiya;

bank asosiy va zaxira ma’lumotlarni qayta ishlash markazlaridagi server xonalari;

Bosh ofis va AB xodimlarining ish joylari;

4) Xavfsizlik va axborotlarni muhofaza qilish departamenti:

bosh ofis va AB binolari va xonalari, u erda joylashgan moddiy boyliklar;

axborot xavfsizligi vositalari, shu jumladan tarmoqlararo ekran, IDPS va VPN vositalari, DLP tizimi, virusga qarshi himoya vositalari, ERI kalitlarini ro‘yxatga olish

markazi, axborotni kriptografik himoyalash vositalari va boshqalar;

5) Lokal tarmoqlarga va ularga kiritilgan tarmoq uskunalariga, MBXO va ularga bo'ysunuvchi BXMdagi ish stansiyalariga, masofaviy kassalarga nisbatan MBXOning axborot texnologiyalari bo'limlari;

6) MBXO va ularga bo'ysunuvchi BXMda joylashgan xonalar, binolar va moddiy boyliklar, masofaviy kassalar, shuningdek u yerda o'rnatilgan shaxsiy axborot xavfsizligi vositalariga nisbatan MBXOning Xavfsizlik va axborotni muhofaza qilish bo'limlari;

7) Aloqa markazi Muvofiqlikni nazorat qilish departamenti bilan birgalikda bank mijozlarining murojaatlari bo‘yicha Call-markaz orqali qabul qilish;

8) Bank boshqaruvining obro‘ va imijiga nisbatan boshqaruvi.

19. Shuningdek, Xavfsizlik va axborotlarni muhofaza qilish departamentining Axborotlarni muhofaza qilish boshqarmasi axborot xavfsizligi hodisalari to'g'risidagi ma'lumotlarni avtomatik ravishda to'playdi:

SIEM axborot xavfsizligi monitoringi va hodisalarni boshqarish tizimlari;

muhim uskunalarning ishlashini monitoring qilish va so'rovlar va bank resurslarining yuklanishini monitoring qilish tizimlari;

tarmoqlararo ekrandan jurnallarni yig'ish va qayta ishlash tizimlari.

20. Axborot xavfsizligi hodisasi aniqlanganda bank xodimi, mutaxassisi yoki tarkibiy bo‘linmasi rahbari bu haqda “ishonch telefoni” orqali Xavfsizlik va axborotlarni muhofaza qilish departamentiga xabar berishi shart.

21. Bankda sodir bo‘lgan axborot xavfsizligini ta’minlash bo‘yicha quyidagi hodisalar deb hisoblanishi kerak:

1) avariya va favqulodda vaziyatlar (texnogen tahdidlar, tabiiy ofatlar, ommaviy namoyishlar va boshqalar);

2) Bank ABT va boshqa axborot tizimlarining ishlashi va ishlashidagi nosozliklar – server va tarmoq uskunalari, dasturiy ta’minotdagi nosozliklar;

3) Bank konfidensial ma’lumotlarining konfidensialligi, yaxlitligi va mavjudligini buzish – konfidensial ma’lumotlarni himoya qilish talablarini buzish;

4) hujum qilish, buzib kirish, sizib chiqish va moddiy zarar yetkazish bo'yicha boshqa ruxsat etilmagan harakatlar - qimmatbaho moddiy boyliklar, mablag'lar, ommaviy axborot vositalari va konfidensial ma'lumotlarni yo'qotish va o'g'irlash faktlari;

5) tashqi tarmoq bilan aloqani yo'qotish;

6) Bankning korporativ tarmog‘ida va lokal tarmoqlarida aloqa uzilishi, tarmoq uskunalaridagi texnik nosozliklar, kabel uzilishi va boshqalar;

7) har qanday sababga ko'ra, texnik nosozlik natijasida ham, inson omili bilan bog'liq xatolar natijasida ham axborot xavfsizligi vositalarining ishdan chiqishi;

8) Bank axborot tizimlari va resurslariga uchinchi shaxslarning ruxsatsiz yoki avtorizatsiyasiz jismoniy yoki mantiqiy kirishi;

9) DoS (Denial of Service) va DDoS (Distributed Denial of Service) xizmat ko‘rsatishni rad etish;

10) himoya vositalari bilan aniqlangan tarmoq hujumlari va bartaraf etish;

11) aniqlangan xavfli viruslar va zararli dasturlar;

12) qurilmalar va tarmoq tugunlarining korporativ yoki lokal tarmoqqa ruxsatsiz ulanishi;

13) himoyalangan binolarga ruxsat etilmagan shaxslarning ruxsatsiz kirishi;

14) ma'lumotlarni to'plash va olib tashlash bo'yicha noqonuniy harakatlar aniqlash;

15) g'ayritabiiy tranzaksiya faoliyati.

22. Axborot xavfsizligi hodisalari aniqlanganda, bank xodimi Xavfsizlik va axborotlarni muhofaza qilish departamentiga quyidagilar haqida xabar berishi shart:

hodisani aniqlash vaqti;

voqea sodir bo'lgan himoyalangan obyekt;

yuzaga keladigan oqibatlar va ularning tabiati;

hodisaning sabablari, agar ular xodimga ma'lum bo'lsa;

voqea haqida ham xabardor bo'lgan shaxslar.

Agar MBXO va unga bo'ysunuvchi BXM, masofaviy kassalarda voqea sodir bo'lgan bo'lsa, ularning xodimlari bu haqda MBXOning Xavfsizlik va axborotni muhofaza qilish bo'limiga xabar berishlari kerak va ular o'z navbatida Xavfsizlik va axborotlarni muhofaza qilish departamentiga hodisa haqida ma'lumot berishlari kerak.

23. Tadbir to‘g‘risida olingan ma’lumotlar asosida Xavfsizlik va axborotlarni muhofaza qilish departamenti tadbirni tahlil qiladi va baholaydi, uning asosida:

hodisani voqea deb tasniflaydi yoki uni axborot xavfsizligi hodisasi deb belgilamaydi;

axborot xavfsizligi hodisasining xavflilik darajasini belgilaydi;

xodimni keyingi harakatlari haqida xabardor qiladi.

Bundan tashqari, voqeani tahlil qilish va baholashda Xavfsizlik va axborotlarni muhofaza qilish departamenti qo'shimcha ma'lumotlarni, shu jumladan monitoring tizimlari, axborot tizimlari va axborotni qayta ishlash va himoya qilish vositalarining hodisalar jurnallaridan foydalangan holda to'playdi. Ushbu qo‘shimcha ma’lumotlar to‘plamiga Axborot texnologiyalari departamenti va boshqa tarkibiy bo‘linmalarning xodimlari jalb etilishi mumkin.

24. Agar hodisa ushbu hujjatning 21-bandida ko'rsatilgan hodisalar ro'yxatiga kiritilgan bo'lsa, u holda Xavfsizlik va axborotlarni muhofaza qilish departamenti ushbu hodisani hodisa sifatida belgilaydi va ularning hisobini yuritadi.

Axborot xavfsizligi hodisalarini hisobga olish axborot xavfsizligi hodisalarini monitoring qilish va boshqarish tizimlari tomonidan ushbu tizimlarning ma'lumotlar bazasida tegishli ma'lumotlarni saqlagan holda amalga oshiriladi.

Axborot xavfsizligi hodisalarini monitoring qilish va boshqarish tizimlari tomonidan aniqlanmagan axborot xavfsizligi hodisalari shakli ushbu nizomning 1-ilovasida belgilangan Axborot xavfsizligi hodisalarining alohida elektron ma’lumotlar bazasida qayd etiladi.

25. Axborot xavfsizligi hodisasini tahlil qilish va baholashda Xavfsizlik va axborotlarni muhofaza qilish departamenti jadvalda belgilangan qoidalarga muvofiq hodisaning muhimlik darajasini belgilaydi.

Axborot xavfsizligi hodisasining muhimlik darajasini aniqlash

Xavf darajasi	Voqea tavsifi	Javob berish mezoni
Yuqori	Muhim himoya obyektida (muhim axborot tizimlari va obyektlari, 3 zonali xavfsizlik obyektlari, muhim konfidensial ma'lumotlar) sodir bo'lgan jiddiy hodisa bank faoliyatining yoki uning muhim texnologik va ishlab chiqarish jarayonlarining to'xtatilishiga yoki to'xtatilishiga olib kelgan yoki natijada shundan bank katta miqdorda moddiy zarar ko'rgan yoki uning obro'si yoki imijiga putur yetkazilgan yoxud bank mijozlariga jiddiy ma'naviy yoki moddiy zarar yetkazilganligi.	Voqea haqida bank rahbariyatini xabardor qilish. Uni bartaraf etish uchun Bankning barcha zarur mablag'lari va resurslarini jalb qilish. Zarur hollarda huquqni muhofaza qiluvchi organlarni jalb qilgan holda hodisa sabablarini o'rganish. Zararni baholash.
O'rta	Muhim bo'lmagan himoya qilinadigan obyektda sodir bo'lgan voqea bankning asosiy ishlab chiqarish vazifalari va funksiyalarini buzmagan holda bankning ayrim texnologik va ishlab chiqarish jarayonlarining to'xtatilishiga yoki to'xtatilishiga olib kelgan yoki bank uchun ahamiyatsiz bo'lgan moddiy zarar yoki individual mijoz yoki sherikka ma'naviy yoki moddiy zarar yetkazish.	Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori va voqea sodir bo'lgan joydagi tarkibiy bo'linma boshlig'ini voqea haqida xabardor qilish. Voqea sodir bo'lgan joyda, uni bartaraf etish uchun tarkibiy bo'linmaning resurslari va vositalaridan foydalanish. Axborot xavfsizligi hodisasini tahlil qilish va baholash.
Past	Himoya obyektining keyingi faoliyatiga ta'sir qilmagan yoki bank va uning mijozlari, sheriklariga moddiy yoki ma'naviy zarar yetkazmagan hodisa.	Xavfsizlik va axborotlarni muhofaza qilish departamentida hodisani hisobga olish. Hodisaning takrorlanishini aniqlash uchun monitoring. Voqea takrorlangan taqdirda, tegishli choralarni ko'rgan holda axborot xavfsizligi hodisalarini tahlil qilish va baholash.

26. "Yuqori" xavflilik darajasiga ega bo'lgan axborot xavfsizligi hodisalari bankning Favqulodda xavfsizlik holatlari reyestrida qayd etilishi kerak, uning shakli ushbu nizomning 2-ilovasida belgilangan.

Ko'rsatilgan jurnal Bankda sodir bo'lgan hodisalar to'g'risidagi ma'lumotlarni to'plash, hisobga olish, ro'yxatga olish uchun mas'ul bo'lgan Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimi tomonidan yuritiladi.

27. Mazkur hujjatning 19-bandida ko'rsatilgan monitoring tizimlarida, shuningdek, bankning axborot xavfsizligi hodisalari ma'lumotlar bazasida sodir bo'lgan hodisalar va axborot xavfsizligi xavflarini baholash bo'yicha statistik

ma’lumotlarni shakllantirish va ushbu ma’lumotlardan tahlil qilish uchun foydalanish uchun ma’lumotlarni saqlash muddati cheklanmaydi.

Bankdagi axborot xavfsizligi hodisalar to‘g‘risidagi ma’lumotlar ham har oyda risklarni boshqarish departamentiga taqdim etiladi.

Bank monitoring tizimlari va axborot xavfsizligi hodisalari ma’lumotlar bazasida saqlangan ma’lumotlarga kirish cheklangan bo‘lishi va faqat Xavfsizlik va axborotlarni muhofaza qilish departamenti xodimlari tomonidan ta’minlanishi kerak.

28. Aniqlangan axborot xavfsizligi hodisasi to'g'risida xabarlarni yig'ish, qayd etish va ro'yxatga olish uchun mas'ul xodim:

bank xavfsizligi departamenti direktori va/yoki bank xavfsizligi boshqarmasi boshlig‘i yoki axborot xavfsizligi boshqarmasi boshlig‘i;

hodisa oqibatida zarar ko‘rgan bankning ishlab chiqarish maydonchasi yoki texnologik jarayoni uchun mas’ul bo‘lgan tarkibiy bo‘linma rahbariyati;

qo'riqlanadigan obyektni saqlash uchun mas'ul bo'lgan tarkibiy bo'linma yoki mutaxassis (administrator) rahbariyati.

Agar hodisa oqibatlari “yuqori” xavf darajasiga ega bo‘lsa, Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori bu haqida bank rahbariyatiga xabar beradi.

29. Axborot xavfsizligi hodisasi haqida xabar berishda quyidagi ma'lumotlar xabar qilinishi kerak:

hodisani aniqlash vaqti;

voqea sodir bo'lgan himoya obyekti;

hodisaning xavflilik darajasi;

hodisaning tabiati va uning oqibatlari;

voqea sabablari va (yoki) aybdorlar, agar ular ma'lum bo'lsa;

voqea munosabati bilan qilingan harakatlar.

30. Tashqi manfaatdor tashkilotlarni xabardor qilish to‘g‘risidagi qaror bank rahbariyati tomonidan qabul qilinadi.

Uchinchi tashkilotlarni xabardor qilish uchinchi tashkilot darajasi va oqibatlari xususiyatidan kelib chiqqan holda bank xavfsizligi va axborotlarni muhofaza qilish departamenti direktori yoki boshqa tarkibiy bo‘linmalari rahbarlari zimmasiga yuklanadi.

31. Bank Axborot xavfsizligi hodisalariga qarshi kurashish guruhi rahbari bo‘lgan Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori tahdidni mahalliylashtirish yoki tahdidning "yuqori" yoki "o'rta" xavf darajasi ta’sirini bartaraf etish bo‘yicha ishlarni tashkil etadi.

Bank rahbariyati bilan kelishilgan holda ushbu ishlarga boshqa tarkibiy bo‘linmalar va mutaxassislar jalb qilinishi mumkin.

MBXO va unga bo'ysunuvchi BXMda, masofaviy kassalar, Xavfsizlik va axborotni muhofaza qilish bo’limi, shuningdek, MBXOdagi Axborot texnologiyalari bo'limi tahdidni mahalliylashtirish yoki tahdid ta'sirini bartaraf etishda ishtirok etadi.

32. Tarmoq hujumlari va zararli dasturlarni yuqtirish holatlarida quyidagi tahdidlarni oldini olish choralarini ko'rish kerak:

zaxiradagi tashqi aloqa kanallarini faollashtirish;

tashqi tarmoqdan uzilish;

IP-manzilni o'zgartirish;

qurilmani korporativ yoki lokal tarmoqdan uzish va h.k.

33. Texnik nosozliklar bo'lsa, ishlashni tiklash bo'yicha quyidagi ishlar amalga oshiriladi, xususan:

zaxira foydalanish vositasi;

ma'lumotlarni qayta tiklash;

uskunaning sozlamalarini yoki ishlash rejimini o'zgartirish;

dasturlarni qayta ishga tushirish yoki qayta o'rnatish;

uskuna komponentini ishga yaroqli bilan almashtirish;

ta'mirlash ishlarini olib borish.

34. Qayta tiklash ishlari himoya qilinadigan obyektni tiklash bo'yicha favqulodda rejaga muvofiq amalga oshirilishi kerak.

35. Voqealarni bartaraf etish va uning faoliyatini tiklash bo'yicha ishlarning borishi to'g'risida vaqti-vaqti bilan Xavfsizlik va axborotlarni muhofaza qilish departamentiga xabar berilishi kerak.

Agar hodisani bartaraf etish va tiklash Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori tomonidan nazorat qilinsa, ularni amalga oshirishning borishi unga xabar qilinadi.

36. Hodisani tahlil qilish va hodisa sabablarini aniqlash Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan manfaatdor tarkibiy bo‘linmalar va mutaxassislarni jalb qilgan holda amalga oshiriladi.

37. Agar hodisa natijasida bank zarar ko‘rgan bo‘lsa, u holda voqeani tahlil qilishda ko‘rilgan zarar va yo‘qotishlar miqdori aniqlanishi kerak. Ko'rilgan zararni yoki zarar miqdorini aniqlash uchun tahlilga Buxgalteriya hisobi va moliyaviy menejment departamenti xodimlari jalb qilinishi mumkin.

38. Tahlil natijalariga ko'ra Xavfsizlik va axborotlarni muhofaza qilish departamenti hisobot tuzadi, unga quyidagilar kiradi:

voqea sodir bo'lishiga olib kelgan tahdidlarning xususiyatlari, so'nggi davrdagi bunday tahdidlarning paydo bo'lish chastotasi;

hodisa sabablari va tahdid manbalari;

hodisa uchun zaifliklardan foydalanilgan;

hodisa yoki uning miqyosi va oqibatlariga olib kelgan mavjud xato va kamchiliklar;

hodisaning sababi va/yoki oqibatlari uchun javobgarlik;

oqibatlarning xarakteri, yetkazilgan zarar yoki zarar miqdori;

tahdidni bartaraf etish va tiklash bo'yicha ko'rilgan harakatlar, shuningdek, ushbu harakatlarning natijasi;

hodisa oqibatlarini bartaraf etish bo‘yicha ko‘rilgan yoki amalga oshirilishi lozim bo‘lgan chora-tadbirlar va harakatlar;

hodisaning takrorlanishining oldini olish bo'yicha chora-tadbirlar va ko'riladigan harakatlar.

Ushbu bayonnoma Axborot xavfsizligi hodisalariga qarshi kurash guruhi xodimlari va hodisani tahlil qilishda ishtirok etgan boshqa shaxslar tomonidan imzolanadi hamda bank rahbariyatiga taqdim etiladi.

39. Hodisa tahlili bo‘yicha hisobotni kelishishda Xavfsizlik va axborotlarni muhofaza qilish departamenti bankning hodisa oqibatlarini bartaraf etish va voqea takrorlanishining oldini olishga qaratilgan chora-tadbirlarni ko‘rish to‘g‘risida qaror tayyorlaydi.

40. Voqea sodir etganlikda aybdor shaxslarni javobgarlikka tortish maqsadida bank rahbariyati hodisa yuzasidan surishtiruv ishlarini olib borish jarayonini boshlaydi.

41. Voqealarni tekshirish quyidagi maqsadlarda amalga oshirilishi kerak:

jinoyatchilarni aniqlash;

aybdorlarni javobgarlikka tortish uchun dalillar va hujjatlarni to'plash;

aybdorning harakatlarining xarakterini aniqlash - qasddan, tasodifan, maqsadli va boshqalar.

42. Voqea yuzasidan tekshiruv o‘tkazish uchun Xavfsizlik va axborotlarni muhofaza qilish departamenti tomonidan bank rahbariyatining tarkibiga muvofiq maxsus guruh tuziladi.

43. Voqea bo'yicha tergovning bir qismi sifatida tergov guruhlari quyidagi huquqlarga ega:

voqea sodir bo'lgan bank binosiga, shu jumladan xodimlarning ish joyiga yoki zarur dalillarni to'plash uchun boshqa jihozlarga to'g'ridan-to'g'ri kirish;

bank xodimlaridan tekshirishga taalluqli hujjatlar yoki boshqa ma’lumotlarni ko‘rib chiqish va tergov materiallariga kiritish uchun taqdim etishni talab qilish;

bank xodimlaridan hodisada bevosita yoki bilvosita ishtirok etganlik fakti to‘g‘risida tushuntirish xati yozishni talab qilish;

voqeada bevosita yoki bilvosita ishtirok etish fakti bo'yicha bank xodimlarini shaxsiy suhbatga chaqirish.

44. Voqealarni tergov qilishda bank xodimlari tergov guruhi vakilining iltimosiga binoan quyidagilarni ta'minlashlari shart:

tergov guruhi vakili tomonidan so'ralgan ma'lumotlar;

yozma tushuntirishlar;

bank binolariga, shu jumladan uning ish joyiga, shuningdek, boshqa jihozlarga kirish.

45. Huquqni muhofaza qiluvchi organlar aybdorlarni jinoiy javobgarlikka tortish uchun hodisalarni tekshirishga jalb qilinishi mumkin.

Tergovga huquqni muhofaza qiluvchi organlarni jalb etish to‘g‘risidagi qaror bank rahbariyati tomonidan qabul qilinadi.

46. Voqealarni tekshirish natijalari bank rahbariyatiga taqdim etiladi.

47. Aybdorlarga nisbatan jazo choralari bank rahbariyati tomonidan qonun hujjatlariga va mehnat shartnomasiga muvofiq amalga oshiriladi.

VI. Tashqi tashkilotlar bilan o'zaro hamkorlik qilish tartibi

48. Bank axborot xavfsizligi hodisalarini boshqarishda quyidagi tashqi tashkilotlar bilan hamkorlik qilishi mumkin:

1) hodisalarga ko’rilgan choralar va ularni amalga oshirilishi to’g’risida xabardor qilish bo’yicha yuqori tashkilotlar (Markaziy bank va boshqalar);

2) “Kiberxavfsizlik markazi” DUKni, hodisalar to’g’risida xabardor qilish, ularni bartaraf etish, oqibatlarini bartaraf etish va takrorlanishining oldini olish bo’yicha maslahat va tavsiyalar olish;

3) Bank o’z faoliyati davomida o’zaro hamkorlikda bo’lgan manfaatdor tashqi tashkilotlar (sheriklar, operatorlar, xizmat ko’rsatuvchi provayderlar, yetkazib beruvchilar) sodir bo’lgan hodisalar to’g’risida xabardor qilish, shunga o’xshash hodisalarning takrorlanishini bartaraf etish, oqibatlarini bartaraf etish va oldini olish bo’yicha birgalikdagi qo’shma chora-tadbirlar ishlab chiqish;

4) jinoyat ishlarini qo’zg’atish va hodisalarni o’rganishda ishtirok etish nuqtai nazaridan huquqni muhofaza qiluvchi organlar;

5) favqulodda holatga olib kelgan hodisalar to’g’risida xabardor qilish, ularning oqibatlarini bartaraf etishda ishtirok etish va ularning sabablarini tekshirish nuqtai nazaridan favqulodda vaziyatlar organlari;

6) hodisalar haqida xabar berish va ularni bartaraf etish, kamchiliklarni bartaraf etish yoki xizmatlarni qayta tiklash to’g’risida xabardor qilish nuqtai nazaridan, tashkilot mijozlariga.

49. Hodisa haqida xabardor qilish, hodisalarni boshqarish jarayoniga jalb qilish nuqtai nazaridan tashqi tashkilotlar bilan o’zaro hamkorlik to’g’risidagi qaror bank rahbariyati tomonidan qabul qilinadi.

50. Hodisa sodir bo’lgan taqdirda bank bosh ofisining axborot xavfsizligi administratori, O’zbekiston Respublikasi davlat va xo’jalik boshqaruvi organlari axborot xavfsizligini ta’minlash bilan bog’liq hodisalarga javob qaytarish, tekshirish va ularning oldini olish uchun “Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining o’zaro hamkorligi to’g’risida” gi nizomga muvofiq “Kiberxavfsizlik markazi” DUK bilan o’zaro hamkorlik qilishi shart.

51. Axborot xavfsizligi administratori “Kiberxavfsizlik markazi” DUK bilan o’zaro hamkorlik doirasida quyidagilarga majburdir:

o’z vaqtida, lekin hodisa aniqlangandan keyin 2 (ikki) soatdan kechiktirmay “Kiberxavfsizlik markazi” DUKni xabardor qilish;

“Kiberxavfsizlik markazi” davlat unitar korxonasidan hodisa to’g’risida xabar qabul qilingan taqdirda, hodisa to’g’risidagi ma’lumotlarning yaxlitligi va ishonchliligini ta’minlash choralarini ko’rish;

hodisa to’g’risidagi ma’lumotlarni “Kiberxavfsizlik markazi” davlat unitar korxonasiga taqdim etish;

hodisaning oldini olish bo’yicha ko’rilayotgan chora-tadbirlar to’g’risida “Kiberxavfsizlik markazi” DUKga ma’lum qilish.

52. Hodisa oqibatlarini bartaraf etish bo’yicha zarur choralar ko’rilgandan 3 (uch) ish kunidan so’ng bank bosh ofisi axborot xavfsizligi administratori “Kiberxavfsizlik markazi” DUKga bajarilgan ishlar to’g’risidagi hisobot bilan tuzatishlar ishlari bo’yicha ma’lumotnoma taqdim etadi..

53. Bank rahbariyatining roziligi bilan “Kiberxavfsizlik markazi” DUK axborot xavfsizligi hodisalarini tekshirishga jalb etilishi mumkin.

54. “Kiberxavfsizlik markazi” DUK tomonidan Bankka axborot xavfsizligi bilan bog‘liq hodisalarning takrorlanishining oldini olish maqsadida xat shaklida taqdim etilgan taklif va tavsiyalar asosida Xavfsizlik va axborotlarni muhofaza qilish

departamenti ularni amalga oshirish rejasini tayyorlaydi va uning bajarilishini ta’minlaydi.

55. Huquqni muhofaza qilish organlari axborot xavfsizligi bilan bog’liq og’ir oqibatlarga olib keladigan hodisalarni tekshirishda huquqbuzarlarni jinoiy javobgarlikka tortish uchun jalb etilishi kerak.

56. Agar hodisa favqulodda vaziyatga olib kelgan bo’lsa (yong’in, suv toshqini, binoning qulashi va boshqalar), u holda bank favqulodda vaziyatlar organlarini ularning oqibatlarini bartaraf etish va sabablarini tekshirishga jalb qilish uchun ushbu hodisalar haqida xabardor qiladi.

57. Hodisalarning yuzaga kelishi bankning hamkorlari, yetkazib beruvchilari (telekommunikatsiya operatori va boshqalar) va boshqa manfaatdor tashkilotlar bilan o’zaro munosabatlari jarayonlarining buzilishiga olib kelishi mumkin. Shu bilan birga, o’zaro munosabat jarayonlarining buzilishi Bankda sodir bo’lgan hodisalar bilan ham, tegishli tashkilot tomonidan sodir bo’lgan hodisalar bilan ham bog’liq bo’lishi mumkin.

Bunday holatlar yuzaga kelganda, bank sodir bo’lgan hodisalar to’g’risida ularni xabardor qilish, oqibatlarini bartaraf etish va yo’q qilish bo’yicha birgalikdagi harakatlarni ishlab chiqish, qayta tiklash ishlarining olib borishi to’g’risida xabardor qilishi va buzilgan o’zaro munosabat jarayonlarini tiklash maqsadida ular bilan o’zaro hamkorlik qilishi shart.

58. Agar noxush holatlar bank xizmatlarini ko‘rsatishning imkonsizligiga olib kelgan bo‘lsa, bank bu haqida bank mijozlarini xabardor qilishi shart.

59. O‘zaro faoliyat yurituvchi uchinchi tomon tashkilotlari va bank mijozlari bilan hodisalarni bartaraf etish masalalari bo‘yicha aloqalar bankning tarkibiy bo‘linmalari tomonidan amalga oshiriladi, ularning vakolatiga ular bilan o‘zaro hamkorlik kiradi.

Axborot xavfsizligi hodisalariga javob berish qoidalariga 1-ilova

“O‘zsanoatqurilishbank” ATB axborot xavfsizligi hodisalari elektron ma’lumotlar bazasi shakli

№	Hodisa sodir bo'lgan sana va vaqt	Bank bo'linmasining nomi	Himoya obyektining nomi	Tahdidni amalga oshirish turi va usuli	Hodisa oqibatlarining xarakteri	Moddiy zarar qiymati (so'm)	Tarkibiy bo'limi va uchinchi shaxslar hodisa haqida xabardor qilinganligi	Hodisa haqida xabar berilgan sana va vaqt	Hodisani bartaraf etish bo'yicha ko'rilgan choralar	Hodisalarini bartaraf etish sanasi va vaqti
1	2	3	4	5	6	7	8	9	10	11

Axborot xavfsizligi hodisalariga javob
berish qoidalari 2-ilova

“O‘zsanoatqurilishbank” ATB favqulodda vaziyatlarni hisobga olish jurnali shakli

№	Hodisa sodir bo'lgan sana va vaqt	Hodisa sodir bo'lgan himoyalangan obyektning nomi	Tahdidni amalga oshirish turi va usuli	Hodisa oqibatlarining tabiati	Hodisa hal qilingan sana va vaqt	Mas'ul shaxsning imzosi
1	2	3	4	5	6	7

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga 19-
ilova

ATB Axborot xavfsizligi siyosati bilan tanishish jurnali

№	F.I.Sh.	Bo‘linma (bo‘limi)/lavozimi	Sana	Imzo

“O‘zsanoatqurilishbank” ATBning
axborot xavfsizligi siyosatiga
20-ilova

Bankning tashkiliy tuzilmasi va bank xizmatlari markazlari ro'yxati

1	Respublika (Bosh ofis) Bosh ofis qoshidagi Amaliyot boshqarmasi	
2	O’zSQB qoshidagi Amaliyot boshqarmasi	Joyda onlayn BXM
	Qoraqalpog‘iston Respublikasi	
3	O’zSQB qoshidagi Amaliyot boshqarmasi	Qoraqalpog‘iston mintaqaviy BXO
4	Qoraqalpog‘iston mintaqaviy BXO	Innovatsiya BXM
5	Qoraqalpog‘iston mintaqaviy BXO	Bo‘ston BXM
6	O’zSQB qoshidagi Amaliyot boshqarmasi	Taxiatosh BXM
7	Taxiatosh BXM	Xo‘jayli BXM
8	O’zSQB qoshidagi Amaliyot boshqarmasi	Qo‘ng‘irot BXM
	Andijon viloyati	
9	O’zSQB qoshidagi Amaliyot boshqarmasi	Andijon mintaqaviy BXO
10	O’zSQB qoshidagi Amaliyot boshqarmasi	Bunyodkor BXM
11	Bunyodkor BXM	Barkamol BXM
12	Bunyodkor BXM	Barhayot BXM
13	O’zSQB qoshidagi Amaliyot boshqarmasi	Xonobod BXM
	Buxoro viloyati	
14	O’zSQB qoshidagi Amaliyot boshqarmasi	Buxoro mintaqaviy BXO
15	Buxoro mintaqaviy BXO	Mustaqillik BXM
16	Buxoro mintaqaviy BXO	Markaziy bozor BXM
17	O’zSQB qoshidagi Amaliyot boshqarmasi	To‘qimachilik BXM
18	To‘qimachilik BXM	Taraqqiyot BXM
19	O’zSQB qoshidagi Amaliyot boshqarmasi	Qorovulbozor BXM
20	Qorovulbozor BXM	Kogon BXM
	Jizzax viloyati	
21	O’zSQB qoshidagi Amaliyot boshqarmasi	Jizzax mintaqaviy BXO
22	O’zSQB qoshidagi Amaliyot boshqarmasi	So‘g‘diyona BXM
	Navoiy viloyati	
23	O’zSQB qoshidagi Amaliyot boshqarmasi	Navoiy mintaqaviy BXO
24	Navoiy mintaqaviy BXO	Ishonch BXM
25	Navoiy mintaqaviy BXO	Saxovat BXM
26	Navoiy mintaqaviy BXO	Darxon BXM
27	Navoiy mintaqaviy BXO	Nizomiy BXM
	Namangan viloyati	
28	O’zSQB qoshidagi Amaliyot boshqarmasi	Namangan mintaqaviy BXO
	Samarqand viloyati	
29	O’zSQB qoshidagi Amaliyot boshqarmasi	Samarqand mintaqaviy BXO
30	O’zSQB qoshidagi Amaliyot boshqarmasi	Amir Temur BXM
31	Amir Temur BXM	Turkiston BXM
	Sirdaryo viloyati	

32	O’zSQB qoshidagi Amaliyot boshqarmasi	Sirdaryo mintaqaviy BXO
33	Sirdaryo mintaqaviy BXO	Birlashgan BXM
34	Sirdaryo mintaqaviy BXO	Yangiyer BXM
	Surxondaryo viloyati	
35	O’zSQB qoshidagi Amaliyot boshqarmasi	Surxondaryo mintaqaviy BXO
36	Surxondaryo mintaqaviy BXO	Jarqo‘rg‘on BXM
37	O’zSQB qoshidagi Amaliyot boshqarmasi	Sariosiyo BXM
38	Sariosiyo BXM	Denov BXM
39	Sariosiyo BXM	Sharg‘un BXM
	Farg‘ona viloyati	
40	O’zSQB qoshidagi Amaliyot boshqarmasi	Farg‘ona mintaqaviy BXO
41	Farg‘ona mintaqaviy BXO	Marg‘ilon BXM
42	Farg‘ona mintaqaviy BXO	Farovon BXM
43	O’zSQB qoshidagi Amaliyot boshqarmasi	Kirguli BXM
44	O’zSQB qoshidagi Amaliyot boshqarmasi	Qo‘qon BXM
45	Qo‘qon BXM	Movarounnahr BXM
	Xorazm viloyati	
46	O’zSQB qoshidagi Amaliyot boshqarmasi	Xorazm mintaqaviy BXO
47	Xorazm mintaqaviy BXO	Urganch BXM
48	Xorazm mintaqaviy BXO	Xiva BXM
49	Xorazm mintaqaviy BXO	To‘proqqa’la BXM
	Qashqadaryo viloyati	
50	O’zSQB qoshidagi Amaliyot boshqarmasi	Qashqadaryo mintaqaviy BXO
51	Qashqadaryo mintaqaviy BXO	Qarshi BXM
52	Qashqadaryo mintaqaviy BXO	Shahrisabz BXM
53	Qashqadaryo mintaqaviy BXO	Koson BXM
54	Qashqadaryo mintaqaviy BXO	Baraka BXM
55	O’zSQB qoshidagi Amaliyot boshqarmasi	Muborak BXM
	Toshkent viloyati	
56	O’zSQB qoshidagi Amaliyot boshqarmasi	Toshkent viloyati mintaqaviy BXO
57	O’zSQB qoshidagi Amaliyot boshqarmasi	Angren BXM
58	O’zSQB qoshidagi Amaliyot boshqarmasi	Olmaliq BXM
59	Olmaliq BXM	Bo‘ka BXM
60	Olmaliq BXM	Piskent BXM
61	O’zSQB qoshidagi Amaliyot boshqarmasi	Chirchiq BXM
62	O’zSQB qoshidagi Amaliyot boshqarmasi	Qibray BXM
63	Qibray BXM	Salar BXM
64	O’zSQB qoshidagi Amaliyot boshqarmasi	Bekobod BXM
	Toshkent shahri	
65	O’zSQB qoshidagi Amaliyot boshqarmasi	Toshkent shahar mintaqaviy BXO
66	Toshkent shahar mintaqaviy BXO	Humoyun BXM
67	Toshkent shahar mintaqaviy BXO	Besh yog‘och BXM
68	O’zSQB qoshidagi Amaliyot boshqarmasi	Olmazor BXM
69	O’zSQB qoshidagi Amaliyot boshqarmasi	Mirzo Ulug‘bek BXM
70	O’zSQB qoshidagi Amaliyot boshqarmasi	Shahriston BXM
71	Shaxriston BXM	Bektemir BXM

72	O’zSQB qoshidagi Amaliyot boshqarmasi	Sergeli BXM
73	O’zSQB qoshidagi Amaliyot boshqarmasi	Mirobod BXM
74	O’zSQB qoshidagi Amaliyot boshqarmasi	Uchtepa BXM
75	Uchtepa BXM	O’rikzor BXM
76	Uchtepa BXM	Qurilish shaharchasi BXM
77	O’zSQB qoshidagi Amaliyot boshqarmasi	Qatortol BXM
78	O’zSQB qoshidagi Amaliyot boshqarmasi	Chilonzor BXM
79	Chilonzor BXM	Zargarlik BXM
80	Chilonzor BXM	Lutfiy BXM
81	O’zSQB qoshidagi Amaliyot boshqarmasi	Yashnobod BXM
82	Yashnobod BXM	Oybek BXM
83	O’zSQB qoshidagi Amaliyot boshqarmasi	Al-Xorazmiy BXM
84	Al-Xorazmiy BXM	Karvon bozor BXM
85	Al-Xorazmiy BXM	Qurilish mollari bozori BXM
86	Al-Xorazmiy BXM	Izza qurilish mollari BXM
87	O’zSQB qoshidagi Amaliyot boshqarmasi	Rakat BXM
88	O’zSQB qoshidagi Amaliyot boshqarmasi	Labzak BXM
89	Labzak BXM	Abu Saxiy BXM
90	O’zSQB qoshidagi Amaliyot boshqarmasi	Yunusobod BXM

Axborotlashtirish obyektlari faoliyati uchun javobgarlikni taqsimlanishi

Axborotlashtirish obyektining nomi	Mas'ullar
Bank korporativ tarmog‘i, shu jumladan tarmoq uskunalari (marshrutizatorlar, kommutatorlar) aloqa kanallari; Korporativ tarmoqni tashqi tarmoqlar va axborot tizimlariga ulash uchun tashqi kanallar; IP telefoniya tizimi; Videokonferensiya aloqa tizimi;	Axborot texnologiyalari departamenti direktori Aloqa va telekommunikatsiya bo’limi boshlig’i Axborot texnologiyalari departamenti; Korporativ tarmoq administratori.
Korporativ elektron pochta tizimi.	Axborot texnologiyalari departamenti direktori Aloqa va telekommunikatsiya bo’limi boshlig’i Axborot texnologiyalari departamenti; Elektron pochta tizimi administratori.
Korporativ tarmog'i domen server nazorati.	Axborot texnologiyalari departamenti direktori Aloqa va telekommunikatsiya bo’limi boshlig’i Axborot texnologiyalari departamenti; Active Directory tizimi administratori.
Bosh ofis va AB lokal tarmog'ining tarmoq uskunalari, asosiy va zaxira ma'lumotlarni qayta ishlash markazlari	Axborot texnologiyalari departamenti direktori Aloqa va telekommunikatsiya bo’limi boshlig’i Axborot texnologiyalari departamenti;
Bosh ofis va AB fayl serveri.	Axborot texnologiyalari departamenti direktori Aloqa va telekommunikatsiya bo’limi boshlig’i Axborot texnologiyalari departamenti; Active Directory tizimi administratori.
Lotus banklararo elektron pochta tizimi; Internet-banking tizimi; EHAT tizimi.	Axborot texnologiyalari departamenti direktori; Axborot texnologiyalari departamenti Raqamli texnologiyalar va masofaviy bank tizimini qo‘llab-quvvatlash bo‘limi boshlig‘i.
Mobil banking tizimi.	Axborot texnologiyalari departamenti direktori; Dasturiy ta'minotni ishlab chiqish va joriy etish guruhi rahbari.
Bank ABT	Axborot texnologiyalari departamenti direktori; Axborot texnologiyalari departamentining ABT rivojlantirish va qo‘llab-quvvatlash bo‘limi boshlig‘i. Tizim administratori; Buxgalteriya hisobi va moliyaviy menejment departamenti direktori; ABT tizim administratori.
CRM tizimi	Axborot texnologiyalari departamenti direktori; Axborot texnologiyalari departamentining ABT rivojlantirish va qo‘llab-quvvatlash bo‘limi boshlig‘i. Tizim administratori;
ELMA BPM tizimi	Axborot texnologiyalari departamenti direktori; Axborot texnologiyalari departamentining tahliliy hisobotlar guruhi rahbari; Axborot texnologiyalari departamenti Raqamli texnologiyalar va masofaviy bank tizimini qo‘llab-

	quvvatlash bo‘limi boshlig‘i..
CROBS tizimi	Axborot texnologiyalari departamenti direktori; Dasturlash bo'limi boshlig'i. Tizim administratori.
SAP tizimi	Axborot texnologiyalari departamenti direktori; Tashqi tizimlar bilan integratsiyani qo‘llab-quvvatlash bo‘limi boshlig‘i. Tizim administratori.
DWH tizimi	Axborot texnologiyalari departamenti direktori; Axborot texnologiyalari departamentining ABT rivojlantirish va qo‘llab-quvvatlash bo‘limi boshlig‘i. Tizim administratori
Way4 protsessing tizimi	Bank kartalari tizimini qo‘llab-quvvatlash departamenti direktori.
Bank axborot tizimlarining amaliy serverlari va ma’lumotlar bazalari.	Axborot texnologiyalari departamenti direktori; Axborot texnologiyalari departamenti Server va ma’lumotlar bazasini boshqarish bo‘limi boshlig‘i.
Rasmiy web-sayt va korporativ intranet web-sayti	Axborot texnologiyalari departamenti direktori; Axborot texnologiyalari departamenti web-saytlarni ishlab chiqish, Internet va onlayn resurslarni boshqarish guruhi rahbari.
Tarmoqlararo ekran va IDPS vositalari; PAM tizimi.	Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori; Xavfsizlik va axborotlarni muhofaza qilish departamenti; Tarmoqlararo ekran administratori va PAM tizimi administratori.
Antivirus himoya vositalari.	Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori; Xavfsizlik va axborotlarni muhofaza qilish departamenti Elektron kalit hisobi bo‘limi boshlig‘i; Antivirus himoyasi administratori.
Bank ERI kalitlarini ro‘yxatga olish markazi; VPN vositalari; Xavfsiz tarmoq ulanishlarini tashkil etish.	Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori; Xavfsizlik va axborotlarni muhofaza qilish departamenti Elektron kalit hisobi bo‘limi boshlig‘i; ERI kalitlarini ro'yxatga olish markazi administratori.
Axborot xavfsizligi hodisalarini kuzatish va boshqarish tizimlari - SIEM, Zabbix va Elastics Logstasch Kibana (ELK); DLP konfidensial ma'lumotlarning chiqib ketishini himoya qilish tizimi.	Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori; Xavfsizlik va axborotlarni muhofaza qilish departamenti Axborot va kartochkalar tizimi xavfsizligi bo’limi boshlig‘i; Hodisalarni monitoring qilish va hisobini yuritish administratori; DLP tizim administratori.
Bosh ofis va ABning ish stansiyalari va boshqa terminal qurilmalari.	Axborot texnologiyalari departamenti direktori; Axborot texnologiyalari departamentining texnik ta’minot va texnik jihozlarni hisobga olish bo‘limi boshlig‘i.
MBXO, BXM, bo'ysunuvchi tarmog'i; MBXO va BXMdagi fayl-server; MBXO, BXM, masofaviy kassalardagi ish stansiyalari va boshqa terminal qurilmalari.	MBXO axborot texnologiyalari bo'limlari boshliqlari.

Kiritildi:

Xavfsizlik va axborotlarni muhofaza qilish departamenti direktori **S.Sergienko**

Kelishildi:

Axborot texnologiyalari departamenti direktori **T.Norov**

Komplaens nazorat departamenti direktori **J.Yusupov**

Risk menejment departamenti direktorining birinchi o'rinbosari **K.Karimov**

Yuridik departament Metodologiya boshqarmasi boshlig'i **S.Raxmatullayev**