2026y. "04" iyun

Reg. № 04-11/28

"TASDIQLANGAN"

"ANOR BANK" Aksiyadorlik jamiyati

Kuzatuv kengashining

2026y. "26" may dagi

25 -sonli yig'ilish bayoni

Kuzatuv kengashi raisi

_____ Nosirov Sh.N

"ANOR BANK" AKSIYADORLIK JAMIYATINING AXBOROT XAVFSIZLIGI SIYOSATI

Toshkent 2026y.

Mundarija

1. UMUMIY QOIDALAR

1.1 Kirish

"ANOR BANK" aksiyadorlik jamiyatining (keyingi o'rinlarda Bank deb ataladi) axborot xavfsizligi siyosati (keyingi o'rinlarda Siyosat deb ataladi) faoliyatni amalga oshirish maqsadida bank rahbariyati tomonidan axborot xavfsizligini ta'minlash bo'yicha qabul qilingan yondashuv va usullarni belgilaydi hamda o'z faoliyatida yo'naltirilishi lozim bo'lgan yuqori darajadagi himoya maqsadlari va vazifalarining tizimlashtirilgan jaroyonidir, shuningdek bankning axborot xavfsizligini boshqarish tizimini (keyingi o'rinlarda – AXBT) qurishning asosiy tamoyillari belgilaydi.

Bank tijorat raqamli bank hisoblanadi va O'zbekiston Respublikasi hududida saytda yoki mobil ilovalar (keyingi o'rinlarda raqamli bank xizmatlari deb yuritiladi) orqali interaktiv tarzda bank xizmatlarini ko'rsatish faoliyatini amalga oshirishga ustuvor ahamiyat beradi.

Bank o'z faoliyatini amalga oshirish uchun raqamli texnologiyalar samarali joriy etilmoqda va qo'llanilmoqda hamda ular asosida bank axborot-kommunikatsiya infratuzilmasi shakllantirilmoqda va rivojlanmoqda.

Axborot xavfsizligini ta 'minlash vazifasi raqamli bank xizmatlarini ko'rsatish, shuningdek O'zbekiston Respublikasi qonun hujjatlari talablariga muvofiq axborot xavfsizligini ta'minlash uchun axborot-kommunikatsiya infratuzilmasining ishonchli va uzluksiz ishlashini ta'minlash zarur bo'lgan sharoitda ustuvor hisoblanadi.

Axborot xavfsizligini ta'minlash bankning axborot resurslari va axborot tizimlarini himoya qilishga qaratilgan har qanday faoliyatni o'z ichiga oladi.

Ushbu siyosat normalari erishishga qaratilgan asosiy maqsad bankning butun faoliyati barqarorligini oshirish uchun bankning butun axborot infratuzilmasi doirasida axborot xavfsizligiga tahdidlarni kamaytirishdir.

Axborot xavfsizligi himoyalangan konfidensial ma'lumotlarning, shu jumladan tijorat va bank sirlari, bankning xodimlari va mijozlarining shaxsiy ma'lumotlari, bank mulkiga oid ma'lumotlarning konfidensialigini, yaxlitligini va foydalana olishlikni ta'minlash, shuningdek, boshqariladigan ma'lumotlarning davomiy va uzluksiz ishlashini ta'minlash nuqtai nazaridan ko'rib chiqiladi hamda bankning axborot tizimlari va resurslari, shu jumladan avtomatlashtirilgan bank tizimi (keyingi o'rinlarda – ABT) mavjud.

Axborot xavfsizligiga siyosatlar, amaliyotlar, protseduralar va tashkiliy tuzilmalarni o'z ichiga olgan bir qator chora-tadbirlarni amalga oshirish va amalga oshirish orqali erishiladi.

Axborot xavfsizligi bo'yicha chora-tadbirlar majmui raqamli bank xizmatlarini ko'rsatish bo'yicha uzluksiz faoliyatni ta'minlash, tahdidlarni amalga oshirishdan zararni minimallashtirish, ularning ta'sirini bashorat qilish va oldini olish, ishbilarmonlik obro'sini saqlab qolish va qonunchilik talablariga rioya qilish

maqsadida axborot (ma'lumotlar) va uning bank axborot-kommunikatsiya infratuzilmasini keng ko'lamli tahdidlardan himoya qilishni ta'minlashi kerak.

Ushbu siyosat bank o'z faoliyatida rahbarlik qiladigan axborot xavfsizligini ta'minlash sohasidagi hujjatlashtirilgan yo'riqnomalar, qoidalar, protseduralar va amaliy usullar to'plamidir.

Ushbu siyosat bankning barcha tarkibiy bo'linmalariga taalluqlidir va bankning barcha xodimlari va mansabdor shaxslari tomonidan bajarilishi majburiydir. Ushbu siyosatning qoidalari bankning bank ichidagi hujjatlarida foydalanish uchun qo'llaniladi.

1.2. Qo'llanilgan me'yoriy hujjatlar

Bankning axborot xavfsizligi siyosati axborotlashtirish obyektlarining axborot xavfsizligini ta'minlash maqsadida quyidagi O'zbekiston Respublikasi me'yoriy hujjatlarga muvofiq ishlab chiqilgan:

1) O'zbekiston Respublikasining 2003 yil 11 dekabrdagi "Axborotlashtirish to'g'risida"gi 560-II – sonli Qonuni;

2) O'zbekiston Respublikasining 2003 yil 30 avgustdagi "Bank siri to'g'risida"gi 530-II-sonli Qonuni;

3) O'zbekiston Respublikasining 2004 yil 29 apreldagi "Elektron hujjat aylanishi to'g'risida"gi 611-II – sonli Qonuni;

4) O'zbekiston Respublikasining 2006 yil 4 apreldagi "Avtomatlashtirilgan bank tizimida axborotni muhofaza qilish to'grisida"gi 30-sonli Qonuni;

5) O'zbekiston Respublikasining 2014 yil 11 sentyabrdagi "Tijorat siri to'g'risida"gi 374-sonli Qonuni;

6) O'zbekiston Respublikasining 2019 yil 2 iyuldagi "Shaxsga doir ma'lumotlar to'g'risida"gi 547-sonli Qonuni;

7) O'zbekiston Respublikasining 2019 yil 1 noyabrdagi "To'lovlar va to'lov tizimlari to'g'risida"gi 578-sonli Qonuni;

8) O'zbekiston Respublikasining 2019 yil 5 noyabrdagi "Banklar va bank faoliyati to'g'risida"gi o'zbekiston respublikasi qonuniga o'zgartish va qo'shimchalar kirATish haqida"gi 580-sonli Qonuni;

9) O'zbekiston Respublikasining 2022 yil 15 apreldagi "Kiberxavfsizlik to'g'risida"gi 764 - Qonuni;

10) O'zbekiston Respublikasining 2022-yil 29-sentabrdagi "Elektron tijorat to'g'risida"gi 792-sonli Qonuni;

11) O'zbekiston Respublikasining 2022-yil 12-oktyabrdagi "Elektron raqamli imzo to'g'risida"gi 793-sonli Qonuni;

12) O'zbekiston Respublikasi Prezidentining 2020 yil 15 iyundagi PF-6007-sonli "O'zbekiston Respublikasining axborot tizimlari va resurslarini himoya qilish davlat tizimini joriy etish chora-tadbirlari to'g'risida" Farmoni;

13) O'zbekiston Respublikasi Prezidentining 2007 yil 3 apreldagi "O'zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil

etish chora-tadbirlari to‘g‘risida”gi 614 – sonli Qarori;

14) O’zbekiston Respublikasi Prezidentining 2011 yil 8 iyuldagi “Milliy axborot resurslarini muhofaza qilish bo‘yicha chora-tadbirlari to‘g‘risida”gi 1572 – sonli Qarori;

15) 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 qarori;

16) O‘zbekiston Respublikasi Prezidentining 2019-yil 14-sentabrdagi PQ-4452-son “Axborot texnologiyalari va kommunikatsiyalarini joriy etish monAToringi tizimini takomillashtirish hamda ularni himoya qilishni tashkil etishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori;

17) O‘zbekiston Respublikasi Prezidentining 2020 yil 15 iyundagi PQ-4751-son “O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi Qarori;

18) O'zbekiston Respublikasi Prezidentining 2021-yil 1-iyuldagi PQ-5170-son “To'lov tizimlari operatorlari, kredAT va to'lov tashkilotlari faoliyatida kiberxavfsizlikni takomillashtirish chora-tadbirlari to'g'risida” Qarori;

19) O‘zbekiston Respublikasi Prezidentining 2023 yil 31 maydagi “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-167-sonli Qarori;

20) O'zbekiston Respublikasi Vazirlar Mahkamasining 1999 yil 26 martdagi “O'zbekiston Respublikasining axborot resurslarini ma'lumotlar uzatish tarmoqlarida, shu jumladan Internet tarmog'ida tayyorlash va tarqatish tartibi to'g'risidagi nizomni tasdiqlash haqida”gi 137-sonli Qarori;

21) O’zbekiston Respublikasi Vazirlar Mahkamasining 2005 yil 22 noyabrdagi “Axborotlashtirish sohasida normativ-huquqiy bazani takomillashtirish to‘g‘risida”gi 256 – sonli Qarori;

22) O’zbekiston Respublikasi Vazirlar Mahkamasining 2011 yil 4 maydagi “Vazirlar Mahkamasining ijro etuvchi apparatida, davlat va xo‘jalik boshqaruvi, mahalliy davlat hokimiyati organlarida yagona himoyalangan elektron pochtani va elektron hujjat aylanishi tizimini joriy etish hamda ulardan foydalanish chora-tadbirlari to‘g‘risida”gi 126-sonli Qarori;

23) O’zbekiston Respublikasi Vazirlar Mahkamasining 2011 yil 7 noyabrdagi “O’zbekiston Respublikasi Prezidentining “Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g‘risida 2011 yil 8 iyuldagi 1572-son qarorini amalga oshirish chora-tadbirlari haqida”gi 296-sonli Qarori;

24) O’zbekiston Respublikasi Vazirlar Mahkamasining 2015 yil 16 oktabrdagi “O’zbekiston Respublikasi axborotlashtirish obyektlarida konfidensial axborot xavfsizligini tashkil etish va ta’minlash tartibi to‘g‘risidagi Nizomni tasdiqlash to‘g‘risida”gi 295 – sonli qarori;

25) O'zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 17-

dekabrdagi "Jismoniy va yuridik shaxslarning markaziy ma'lumotlar bazalarini shakllantirish va elektron hukumat tizimi foydalanuvchilarini identifikatsiyalashning yagona axborot tizimini joriy etish chora-tadbirlari to'g'risida" gi 365-sonli qarori;

26) O'zbekiston Respublikasi Vazirlar Mahkamasining 2019-yil 21-noyabrdagi "O'zbekiston Respublikasi milliy gvardiyasi qo'riqlash bosh boshqarmasi bo'linmasining qo 'riqlash obyektlari ro'yxatini tasdiqlash to'g'risida" 930-sonli qarori;

27) O'zbekiston Respublikasi Vazirlar Mahkamasining 2022 yil 5 oktyabrdagi "Shaxsga doir ma'lumotlarga ishlov berish sohasidagi ayrim normativ-huquqiy hujjatlarni tasdiqlash to'g'risida"gi 570 - sonli Qarori;

28) O'zbekiston Respublikasi Adliya vazirligi tomonidan 2006 yil 14-fevralda 1545-sonli reg davlat ro'yxatidan o'tkazilgan O'zbekiston Respublikasi Markaziy Banki Boshqaruvining "To'lov tizimlari operatorlari va to'lov xizmatlari provayderlarining to'lov tizimlarida axborot xavfsizligini ta'minlash to'g'risidagi nizomni tasdiqlash haqida"gi qarori;

29) O'zbekiston Respublikasi 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 qarori, 2020 yil 10 martda O'zbekiston Respublikasi Adliya vazirligi tomonidan ro'yxatdan o'tkazilgan. Ro'yxat raqami № 3224 (yangi tahriri 2023 yildagi 3224-2-son);

30) O'zbekiston Respublikasi Markaziy banki Boshqaruvining "To'lov tizimlari operatorlari va to'lov xizmatlari etkazib beruvchilarining to'lov tizimlarida axborot xavfsizligini ta'minlash to'g'risidagi nizomni tasdiqlash to'g'risida"gi qarori (Adliya vazirligi tomonidan 2024 yil 21 mayda 3531-son bilan ro'yxatdan o'tkazilgan).

31) O'zbekiston Respublikasi Adliya vazirligida 2023 yil 22 sentyabrda 3458-son bilan ro'yxatga olingan O'zbekiston Respublikasi Davlat xavfsizlik xizmati Raisining 2023 yil 4 sentyabrdagi "O'zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta'minlash darajasini baholash tartibi to'g'risidagi nizomni tasdiqlash haqida" 91-son Buyrug'i;

32) O'zbekiston Respublikasi Adliya vazirligida 2023 yil 15 noyabrda 3477-son bilan ro'yxatga olingan O'zbekiston Respublikasi Adliya vazirligining 2023 yil 14 noyabrdagi "Shaxsga doir ma'lumotlar bazasining mulkdori va (yoki) operatorining shaxsga doir ma'lumotlarga ishlov berilishini hamda ularning himoya qilinishini ta'minlovchi tuzilmaviy bo'linmasi yoki vakolatli shaxsi faoliyatini tashkil etishning namunaviy tartibini tasdiqlash haqida" 19-mh-son Buyrug'i;

33) O'zbekiston Respublikasi Adliya vazirligida 2023 yil 15 noyabrda 3478-son bilan ro'yxatga olingan O'zbekiston Respublikasi Adliya vazirligining 2023 yil 15 noyabrdagi "Shaxsga doir ma'lumotlarga ish tartibini tasdiqlash haqida" 20-mh-son Buyrug'i;

34) O‘zbekiston Respublikasi Bosh vazirining o‘rinbosari davlat sirlarini saqlash bo‘yicha idoralararo komissiya raisi tomonidan 2006 yil 5 dekabrda tasdiqlangan - tarqatilishi cheklangan ma’lumotlarga ega hujjatlar, fayllar va nashrlarni ro‘yxatga olish, ishlov berish va saqlash tartibi to‘g‘risidagi yo‘riqnoma;

35) O‘zMSt 816:2025 “Axborot xavfsizligi, kiberxavfsizlik va konfidentsiallikni himoya qilish. Axborot xavfsizligi siyosatini ishlab chiqish bo‘yicha qo‘llanma” milliy standarti;

36) O’z DSt 1092:2009 “Axborot texnologiyalari. Axborotni kriptografik himoya qilish. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari”;

37) O’z DSt 1108:2011 “Axborot texnologiyalari. Ochiq tizimlarning o'zaro bog'liqligi. Eri ochiq kalAT sertifikati va atribut sertifikatining tuzilishi”;

38) O‘zDSt 1047:2018 “Axborot texnologiyasi. Atamalar va ta’riflar”;

39) O‘zDSt 1109:2013 “Axborot texnologiyasi. Axborotning kriptografik himoyasi. Atamalar va ta’riflar”;

40) O‘z DSt 2927:2015 “Axborot texnologiyalari. Axborot xavfsizligi. Atamalar va ta’riflar”;

41) O‘z DSt 2590:2012 “Axborot texnologiyasi. Milliy axborot tizimini shakllantirish doirasida davlat organlari tomonidan foydalaniladigan axborot tizimlari integratsiyasiga va o‘zaro faoliyatiga ko‘yiladigan talablar”;

42) O‘zDSt 2814:2014 “Axborot texnologiyasi. Avtomatlashtirilgan tizimlar. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo‘yicha tasniflash”;

43) O‘zSt 2815:2014 “Axborot texnologiyasi. Tarmoqlararo ekranlar. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo‘yicha tasniflash”;

44) O‘z DSt 2816:2014 “Axborot texnologiyasi. Axborotni muhofaza qilish vositalarining dasturiy ta’minotini deklaratsiya qilinmagan imkoniyatlar yo‘qligini nazorat qilish darajasi bo‘yicha tasniflash”;

45) O‘zDSt 2817:2014 “Axborot texnologiyasi. Hisoblash texnikasi vositalari. Axborotdan ruxsatsiz foydalana olishdan muhofazalanganlik darajalari bo‘yicha tasniflash”;

46) O‘zDSt 2875:2014 “Datamarkazlar uchun talablar. “Infratuzilma va axborot xavfsizligini ta’minlash” standartidagi telekommunikatsiya obyektlari infratuzilmasining tayyorligi va xavfsizligini ta’minlash;

47) O‘zDSt 3078:2016 “Telekommunikatsiyalar tarmoqlari. Virtual xususiy tarmoqlar (VPN). Umumiy talablar”;

48) O‘z DSt 3243:2017 “Axborot texnologiyasi. Lokal va korporativ hisoblash tarmoqlari. Umumiy texnik talablar”;

49) O’z DSt 3386:2019 (O’z DSt ISO/IEC 27035-1:2016; MOD) “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi insidentlarini boshqarish. 1 qism, Insidentlarni boshqarish prinsiplari”;

50) O’z DSt 3387:2019 (O’z DSt ISO/IEC 27035-2:2016; MOD) “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi insidentlarini

boshqarish. 2 kism. Insidentlarga ta'sir etishni rejalashtirish va unga tayyorlanish bo'yicha rahbariy ko'rsatmalar";

51) O'z DSt ISO/IEC 11770-1:2017 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. KalATlami boshqarish. 1-qism. Asosiy qoidalar";

52) O'z DSt ISO/IEC 13335-1:2009 "Axborot texnologiyalari. Xavfsizlikni ta'minlash usullari. Axborot va kommunikatsiya texnologiyalari xavfsizligini boshqarish. (1-qism). Axborot va kommunikatsiya texnologiyalari xavfsizligini boshqarish konsepsiyasi va modellari";

53) O'z DSt ISO/IEC 15408-1:2016 "Axborot texnologiyalari. Xavfsizlikni ta'minlash usullari. Axborot texnologiyalarining xavfsizligini baholash mezonlari. (1-qism). Kirish va umumiy model";

54) O'z DSt ISO/IEC 15408-2:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot texnologiyalarining xavfsizligini baholash mezonlari. (2-qism). Xavfsizlikning funksional komponentlari";

55) O'z DSt ISO/IEC 15408-3:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot texnologiyalarining xavfsizligini baholash mezonlari. (3-qism). Xavfsizlikka qo'yiladigan ishonch komponentlari";

56) O'z DSt ISO/IEC 27000:2022 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Sharh va lug'at";

57) O'z DSt ISO/IEC 27001:2020 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligini boshqarish tizimlari. Talablar";

58) O'z DSt ISO/IEC 27002:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligini boshqarishning amaliy qoidalari";

59) O'z DSt ISO/IEC 27003:2022 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligini boshqarish tizimini joriy etish bo'yicha qo'llanma";

60) O'zMSt ISO/IEC 27005:2024 "Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni muhofaza qilish. Axborot xavfsizligi xavflarini boshqarish bo'yicha qo'llanma";

61) O'z DSt ISO/IEC 27007:2022 "Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni muhofaza qilish. Axborot xavfsizligini boshqarish tizimlarini audAT qilish bo'yicha rahbariy ko'rsatmalar";

62) O'z DSt ISO/IEC 27008:2022 "Axborot texnologiyalari. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligini boshqarish bo'yicha audATorlar uchun qo'llanma";

63) O'z DSt ISO/IEC 27010:2015 "Axborot texnologiyalari. Xavfsizlikni ta'minlash usullari. Sohalararo va tashkilotlararo kommunikatsiyalarda axborot xavfsizligini boshqarish bo'yicha qo'llanma";

64) O'z DSt ISO/IEC 27014:2018 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligini korporativ boshqarish";.

65) O'z DSt ISO/IEC 27031:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Biznes uzluksizligini ta'minlashga axborot texnologiyalarini tayyorligi bo'yicha rahbariy ko'rsatmalar";

66) O'z DSt ISO/IEC 27032:2017 "Axborot texnologiyasi. Xavfsizlikni

ta'minlash usullari. Kiberxavfsizlik bo'yicha rahbariy ko'rsatmalar";

67) O'z DSt ISO/IEC 27033-1:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Tarmoq xavfsizligi. 1-qism";

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

69) O'z DSt ISO/IEC 27033-1:2016 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Tarmoq xavfsizligi. 4-qism. Xavfsizlik shlyuzlaridan foydalangan holda tarmoqlar o'rtasida xavfsizlikni ta'minlash";

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

71) O'zDSt ISO/IEC 27033-6:2018 "Axborot texnologiyalari. Xavfsizlik usullari. Tarmoq xavfsizligi. 6-qism: Simsiz IP tarmog'iga xavfsiz kirish;

72) O'zDSt ISO/IES 27037:2017 "Axborot texnologiyalari. Xavfsizlik usullari. Raqamli dalillarni aniqlash, to'plash, olish va saqlash bo'yicha ko'rsatmalar";

73) O'z DSt ISO/IEC 27039:2018 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Bostirib kirishni aniqlash tizimlarini tanlash, qo'llash va tizim operatsiyalari";

74) O'z DSt ISO/IEC 27040:2018 "Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Ma'lumotlami saqlash xavfsizligi";

75) Xalqaro to'lov kartalari sanoati (PCI) ma'lumotlar xavfsizligi standarti (DSS) - to'lov kartalari sanoatida axborot xavfsizligi standarti - karta egalari ma'lumotlarining xavfsizligiga qo'yiladigan talablar to'plami;

76) Bank Boshqaruvining 2020-yil 24-sentabrdagi 7 - bayonnomasi bilan tasdiqlangan Bankda kirishni nazorat qilish qoidalari;

77) AT xizmatlarining favqulodda vaziyatlarni boshqarish tartibi Bank Boshqaruvining 2022-yil 22-avgustdagi 26 - bayonnomasi bilan tasdiqlangan;

78) Bank Boshqaruvining 12.02.2022 yildagi 32 - bayonnomasi bilan tasdiqlangan cheklangan taqsimlanmagan ma'lumotlarni (DSP) o'z ichiga olgan hujjatlar va fayllarni hisobga olish, yuritish va saqlash tartibi to'g'risidagi yo'riqnoma;

79) Bank Boshqaruvining 2022-yil 2-dekabrdagi 32 - bayonnomasi bilan tasdiqlangan Tijorat siri (konfidensial) rejimiga rioya qilish to'g'risidagi nizom;

80) Bank Boshqaruvining 2023-yil 16-maydagi 7-1 - bayonnomasi bilan tasdiqlangan "Anor Bank" AJ xodimlarining shaxsiy ma'lumotlarini qayta ishlash tartibi to'g'risidagi nizom.

1.3 Atamalar va ta'riflar

Ushbu siyosatda quyidagi atamalar, ta'riflar va qisqartmalar qo'llaniladi:

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 hodisasi: Axborot xavfsizligining yagona voqeasi yoki bir qator nohush yoki kutilmagan voqealari bo'lib, ushbu voqealar tufayli biznes axborotni kompрometatsiya qilish ehtimoli va axborot xavfsizligiga tahdidlar ehtimoli katta bo'ladi;

autentifikatsiya: foydalanuvchi tomonidan taqdim etilgan identifikatorning axborot resursiga kirish huquqini tekshirish jarayoni; manbaga kirish huquqlarining haqiqiyligini tasdiqlash.

axborotlashtirish obyekti: Turli daraja va maqsadlardagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotni qayta ishlash texnik vositalari, bu vositalar o'rnatilgan va ekspluatatsiya qilinadigan, 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 himoya qilish (axborotni himoya qilish) – himoyalangan ma'lumotlarning tarqalishini, himoyalangan ma'lumotlarga va unga kirishning dasturiy-texnik vositalariga ruxsatsiz va bexosdan ta'sirlanishini oldini olishga qaratilgan faoliyat;

axborot xavfsizligi: ma'lumotlar bazalarining yaxlitligi va barqarorligini (yaxlitlikni buzish), yo'qolish yoki mavjudlik darajasini pasaytirishni ta'minlaydigan axborotni oshkor qilmaslik (konfidensiallikni buzish), uning tashuvchilari va infratuzilmasidan himoya qilish holati;

axborot infratuzilmasi: bu har qanday axborot xizmatlarining ishlashi uchun asos bo'lgan asosiy axborot xizmatlari va tarmoqlari, hisoblash tizimlari, ma'lumotlarni saqlash, qayta ishlash va uzatish tizimlari to'plami.; intellektual mulk-ixtirolar, ishlanmalar, savdo belgilari, firma nomi, tijorat belgilari, bank mulki bo'lgan nomlar va tasvirlar;

axborot xavfsizligi hodisalarini monitoring qilish va boshqarish tizimi xavfsizlik ma'lumotlari va hodisalarni boshqarish (bundan buyon matnda SIEM deb yuritiladi): bu axborot xavfsizligi hodisalarini yig'ish, saqlash, monitoring qilish va boshqarish, hodisalar oqimidan hodisalarni aniqlash va sodir bo'lgan voqealar to'g'risida tahlilchilarni tezkor ravishda xabardor qilish imkonini beradigan tizim;

axborot xavfsizligi voqealari (bundan buyon matnda voqealar matni deb yuritiladi) - xavfsizlik siyosatining buzilishi yoki himoya mexanizmlarining yo'qligi yoki xavfsizlik bilan bog'liq bo'lishi mumkin bo'lgan ilgari noma'lum vaziyatni ko'rsatadigan tizim, xizmat yoki tarmoqning aniqlangan holati;

axborotni kriptografik himoya qilish vositalari (bundan buyon matnda AKHV): bu mustaqil ravishda yoki boshqa tizimlarning bir qismi sifatida ishlay oladigan va uning xavfsizligini ta'minlash uchun ma'lumotlarning kriptografik konversiyasini amalga oshiradigan ma'lumotlarni qayta ishlash tizimlarining dasturiy va texnik elementlari to'plami;

bank siri: bank tomonidan himoyalangan ma'lumotlar:

- o'z mijozlarining (korrespondent) operatsiyalari, hisobvaraqlari va depozitlari to'g'risida;
- mijozingiz (korrespondent) unga bank xizmatlarini ko'rsatish munosabati bilan bank tomonidan olingan;
- mijozning (korrespondent) seyflarida va bank binolarida saqlanayotgan mol-mulkining mavjudligi, xususiyati va qiymati to'g'risida;
- banklararo bitimlar va mijoz (korrespondent) nomidan yoki uning foydasiga tuzilgan bitimlar bo‘yicha;
- banklar o'rtasida bank sirini tashkil etuvchi ma'lumotlarning aylanishi natijasida ma'lum bo'lgan boshqa bankning mijozi (korrespondenti) to'g'risida;

O'zR Markaziy bankining bank telekommunikatsiya tarmog'i (keyingi o'rinlarda BTT deyiladi): markazlashtirilgan nazoratni, bank ma'lumotlarini to'plash va qayta ishlash jarayonini boshqarishni, ish oqimining samaradorligi, ishonchliligi va xavfsizligini ta'minlaydigan resurslarni boshqarish va to'lov tizimining ishlashi uchun texnologiyalar to'plami;

biznes jarayoni: mahsulotlar, xizmatlar ko'rsatish va/yoki muayyan faoliyat turini amalga oshirish bo'yicha texnologik bog'liq operatsiyalar ketma-ketligi;

buzg‘unchi: Axborot tizimi va uning resurslaridan ruxsat etilmagan tarzda foydalana olishdan manfaatdor bo‘lgan va ularni ruxsatsiz olish yoki o‘zgartirish uchun oldindan o‘ylab harakat qilgan shaxs yoki tashkilot;

virtual xususiy tarmoq (VPN): internetga xavfsiz ulanishni o'rnatishga imkon beradigan texnologiya;

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;

kirishni boshqarish va boshqarish tizimi (bundan buyon matnda SKUD deb yuritiladi): dasturiy-apparat texnik nazorati va kirishni boshqarish vositalari to'plami;

hujumlarni aniqlash va oldini olish vositalari (tizimlari) (bundan keyin IDPS matnida): bu faktlarni aniqlaydigan va korporativ tizimga ruxsatsiz kirishga urinishlarning oldini oladigan dasturiy yoki apparat vositalari to'plami.

elektron hujjat aylanishi tizimi (bundan buyon matnda EHAT deb

yuritiladi): bu bank ichida, shuningdek boshqa sherik tashkilotlar va davlat organlari bilan elektron hujjatlarni almashish tizimi bo'lib, u ma'lumotlarni yaratish, tasdiqlash, yuborish, qabul qilish, arxivlash va qayta ishlatishga imkon beradi;

elektron raqamli imzo (bundan buyon matnda ERI deb yuritiladi): bu mualliflik huquqi, hujjatni imzolash vaqti va uning o'zgarmasligi tekshiriladigan elektron hujjatning atributidir.

ma'lumotlar bazasi: Obyektiv shaklda ifodalangan va bu ma'lumotlar elektron hisoblash mashinalari yordamida topiladigan va qayta ishlanadigan tarzda tizimlashtirilgan ma'lumotlar (moddalar, hisob-kitoblar) jami;

ma'lumotlar bazasini boshqarish tizimi (bundan buyon matnda MBBT deb yuritiladi): bu ma'lumotlar bazalarini yaratish, boshqarish, yangilash va tahlil qilish uchun mo'ljallangan dasturiy ta'minot;

ma'lumotlarni qayata ishlash markazi (bundan buyon matnda ma'lumotlar markazi deb yuritiladi): bu kompyuterlar va tegishli apparat vositalari saqlanadigan jismoniy joy;

nazorat kilinadigan 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 inshoatlari, 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;

xavfni qayta ishlash: xavfni o'zgartirish (kamaytirish) bo'yicha chora-tadbirlarni tanlash va amalga oshirish jarayoni;

shaxsga doir ma'lumotlar: aniqlangan yoki aniqlanayotgan jismoniy shaxsning shaxsini aniqlash imkonini beradigan ma'lumotlar.

tahdid: kompyuter xavfsizligining potentsial buzilishi.

tijorat siri: uchinchi shaxslarga noma'lum bo'lganligi sababli ilmiy-texnikaviy, texnologik, ishlab chiqarish, moliyaviy, iqtisodiy va boshqa sohalarda tijorat ahamiyatiga ega bo'lgan, qonuniy asosda erkin foydalanish imkoni bo'lmagan va ushbu ma'lumotlarning egasi chora ko'radigan ma'lumotlar. uning maxfiyligini himoya qilish.

zaiflik: Ma'lumotlarni qayta ishlash tizimidagi kamchilik, undan

foydalanish uning yaxlitligini buzishi va noto‘g‘ri ishlashiga olib kelishi mumkin;

Privilege Access Management (bundan buyon matnda PAM deb yuritiladi) deb nomlanuvchi imtiyozli foydalanuvchi harakatlarini boshqarish tizimi ishlab chiquvchilar va administratorlarga, shu jumladan uchinchi tomon tashkilotlariga kirishni tashkil qilishda mijozning korporativ tarmog'idagi (axborot tizimlari, resurslar va uskunalar) yuqori tanqidiy aktivlarning xavfsizligini ta'minlash uchun mo'ljallangan.qo'llab – quvvatlash va boshqarish ishlarini bajarish.

intellektual mulk-ixtirolar; ishlanmalar, savdo belgilari, firma nomi, tijorat belgilari, bank mulki bo ' lgan nomlar va tasvirlar.

qayd yozuvi - kompyuter tizimida saqlanadigan foydalanuvchi to'g'risidagi ma'lumotlar to'plami, uni aniqlash (autentifikatsiya qilish) va uning shaxsiy ma'lumotlari va sozlamalariga kirishni ta'minlash uchun zarur. Odatda-qayd yozuvi bu login va parollarning kombinatsiyasi;

1.4. Foydalanish sohasi

Bankning axborot xavfsizligi siyosati o‘z faoliyatida amal qiladigan Bank axborot xavfsizligi sohasidagi maqsad va vazifalarni, qoidalar, tartiblar, amaliyot va yo‘riqlarni belgilaydi.

Bankning axborot xavfsizligi siyosati 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.

Ushbu siyosatning talablari Bankning barcha himoyalangan ma'lumotlariga va ushbu ma'lumotlarni yaratish, qayta ishlash, saqlash, uzatish, himoya qilish va yo'q qilish vositalariga nisbatan qo'llaniladi, davlat sirlarini o'z ichiga olgan ma'lumotlar bundan mustasno. Davlat sirlarini o'z ichiga olgan axborotni himoya qilish davlat sirlarini himoya qilish sohasidagi qonun hujjatlariga muvofiq ta'minlanadi.

Bank tarkibiga quyidagilar kiradi:

a) Bosh ofis - Bosh ofisning tarkibiy bo'linmalarini joylashtirish uchun bino, shuningdek 1-qavatda mijozlarga xizmat ko'rsatish punktini tashkil etish (Toshkent shahri, Sayram ko'chasi, 5-yo'l, o'z binosi);

b) IT-ofis-Bosh ofisning IT tarkibiy bo'linmalarini joylashgan bino (Toshkent shahri, Muqimiy ko'chasi, 59-uy, binoda ijara asosida);

v) savdo ofislari-bank mijozlarga xizmat ko'rsatish punktlari;

Bundan tashqari, Bank tarkibiga Bosh ofisda joylashgan asosiy ma’lumotlarni qayta ishlash markazi va "O'zbektelekom" ATS-233 ma'lumotlar markazida tashkil etiladigan zaxira ma’lumotlarni qayta ishlash markazida (Toshkent shahri, Istiqlol ko'chasi, 51) joylashgan.

Bankning asosiy va zaxira ma'lumotlarni qayta ishlash markazini tashkil etish uchun axborotni qayta ishlash va saqlashning o'z vositalaridan (server va ma'lumotlarni saqlash tizimlari) foydalaniladi.

"O'zbektelekom" AK ATS-233 ma'lumotlarni qayta ishlash markazi Bank zaxira ma'lumotlarni qayta ishlash markazini tashkil etish uchun xonalarni ijaraga oladi va ma'lumotlar markazining ishlashini ta'minlash infratuzilmasidan foydalanadi (uzluksiz elektr ta'minoti, konditsionerlik tizimi, yong'inni o'chirish va boshqalar).

Bankning o 'z kuchi bilan ushbu ma' lumotlarni Bank korporativ tarmog'iga va O'zbekiston Respublikasi Markaziy bankining tashqi tarmoqlariga (Internet, bank telekommunikatsiya tarmog 'i (keyingi o' rinlarda BTT deb ataladi) ulash tashkil etiladi.

Ushbu siyosat talablari quyidagilarga nisbatan qo'llaniladi:

a) Bankning barcha axborot tizimlari va resurslari;

b) Bankning barcha xodimlari (shtat, vaqtinchalik, kontrakt bo'yicha ishlaydigan va boshqalar), ularning ish joyi va egallab turgan lavozimidan qat'i nazar;

v) Bank bilan o'zaro aloqada bo'lgan uchinchi shaxslar (bank mijozlari, yetkazib beruvchilar, ijarachilar, pudratchilar, auditorlar, tashrif buyuruvchilar, xizmat ko'rsatuvchi xodimlar, axborot tizimlarining tashqi foydalanuvchilari va boshqalar), ular biron bir sababga ko'ra xona va himoya obyektlariga, Bank shu jumladan axborot resurslari va tizimlariga qonuniy kirish huquqiga ega.

Bank boshqaruvi, tarkibiy bo‘linmalari rahbarlari, shuningdek Axborot xavfsizligi boshqarmasi mazkur siyosat qoidalariga rioya etilishi ustidan muntazam monitoring olib borilishini ta’minlashi shart. Axborot xavfsizligini boshqarishning funksiyalari va vazifalari belgilangan tartibda boshqaruv to'g'risidagi nizomning bir qismi sifatida tasdiqlanadi.

2. BANKDA AXBOROT XAVFSIZLIGINI TA’MINLASH BO’YICHA MAQSAD VA VAZIFALAR

2.1. Bankning axborot xavfsizligini ta’minlash maqsadlari:

- Bankda subyektlarini axborot himoyasiga munosabatlari va Bank xizmatlaridan foydalanuvchilarni (keyingi o‘rinlarda bank mijozlari deb yuritiladi) ma’lumotlarga tasodifiy yoki qasddan xavfsizlik tahdidlari 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;
- O’zbekiston Respublikasi axborot xavfsizligi sohasidagi qonun hujjatlari, yo’riqnomalar va nizomlarga va umumiy 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;

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

- zarur axborot mavjudligini ta 'minlash orqali bank faoliyatining barqarorligini ta' minlash (uning biznesining uzluksizligini ta ' minlash) ;

- iqtisodiy va texnik jihatdan asoslangan, shuningdek zarur va etarli darajada axborot xavfsizligi choralarini qo'llash orqali axborot xavfsizligi tahdidlaridan himoya qilishga muvozanatli yondashuvni shakllantirish.

2.2. Bankda axborot xavfsizligini ta’minlash maqsadlariga erishish uchun axborot xavfsizligini ta’minlash vazifalari:

- Bankda tadbirkorlik, qonunchilik va me’yoriy hujjatlar talablariga muvofiq AXBTni yaratish va rivojlantirish;

- Bank ning 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;

- AXni ta 'minlash bo' yicha normativ-huquqiy bazani ishlab chiqish va takomillashtirish;

- axborot aktivlarini antivirus himoyasini tashkil etish;

- Bank axborotlashtirishning muhim obyektlari xavfsizligi va ishonchli ishlashi darajasini oshirish.

3. AXBOROT XAVFSIZLIGINI TA’MINLASH BO’YICHA ASOSIY QOIDALAR

3.1. Bank ning axborot xavfsizligi siyosati quyidagi asosiy tamoyillarga asoslanadi:

1) qonuniylik - axborot xavfsizligini ta'minlashda qonun hujjatlari va normativ hujjatlar talablariga rioya qilish;

2) jalb qilish – Bank rahbariyati va barcha xodimlari axborot xavfsizligini boshqarish jarayonida ishtirok etadilar;

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

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

5) 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;

6) 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 borish;

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

8) 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;

9) Komplekslik - axborotni himoya qilish usullari va vositalaridan kompleks foydalanish tahdidlarni amalga oshirishning barcha muhim (muhim) kanallarini to'sib qo'yadigan va uning alohida tarkibiy qismlarining bo'g'inlarida zaif tomonlarni o'z ichiga olmaydigan yaxlit himoya tizimini qurishda heterojen vositalardan kelishilgan foydalanishni o'z ichiga oladi;

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

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

12) hisobot berish va hatti-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.

13) o'z vaqtida-axborot xavfsizligini ta'minlash choralarining proaktiv xususiyatini, ya'ni axborotni har tomonlama himoya qilish bo'yicha vazifalarni belgilashni va umuman axborot tizimlarini va ularning axborotni himoya qilish tizimlarini rivojlantirishning dastlabki bosqichlarida axborot xavfsizligini ta'minlash choralarini amalga oshirishni nazarda tutadi, xususan;

14) yetarlilik darajasi - axborot xavfsizligini ta'minlash xarajatlari darajasining axborot resurslarining qiymati va ularni oshkor qilish, yo'qotish, oqish, yo'q qilish va buzib ko'rsatish natijasida yuzaga kelishi mumkin bo'lgan zarar miqdoriga muvofiqligini nazarda tutadi. Amaldagi axborot resurslari xavfsizligini

ta'minlash choralari va vositalari bank axborot tizimining tarkibiy qismlarining ergonomik ko'rsatkichlarini sezilarli darajada yomonlashtirmasligi kerak;

15) shaxsiy javobgarlik-har bir xodimga o'z vakolatlari doirasida axborot va uni qayta ishlash tizimining xavfsizligini ta'minlash uchun javobgarlikni o'z zimmasiga oladi. Ushbu printsipga muvofiq, xodimlarning huquq va majburiyatlarini taqsimlash shunday tuzilganki, har qanday qoidabuzarlik sodir bo'lgan taqdirda, aybdorlar doirasi aniq ma'lum yoki minimallashtiriladi.

3.2. Bank axborot xavfsizligini ta'minlash bo'yicha o'ziga yuklangan vazifalarni amalga oshirish jarayonida:

- Bank bank axborot-kommunikatsiya infratuzilmasi axborot xavfsizligini ta'minlash jarayonlarini tartibga soluvchi normativ-huquqiy bazani shakllantiradi;
- Bankning axborot va boshqa himoya qilish obyektlarini belgilaydi va toifalarga ajratadi;
- axborot xavfsizligiga tahdidlarni xolis va har tomonlama tahlil qilish va prognozlash, tahlil qilish va xavflarni baholashni amalga oshiradi;
- Bankning bank axborot-kommunikatsiya infratuzilmasida axborot xavfsizligini ta'minlash bo'yicha talablar va chora-tadbirlar ishlab chiqadi;
- axborot xavfsizligiga tahdidlarning oldini olish, ularni qaytarish va zararsizlantirishga qaratilgan chora-tadbirlar kompleksini amalga oshirish bo'yicha zarur bo'linmalar ishini tashkil etadi;
- axborot xavfsizligiga tahdidlarning oldini olish, ularni qaytarish va zararsizlantirishga qaratilgan chora-tadbirlar kompleksini amalga oshirish bo'yicha zarur bo'linmalar ishini tashkil qiladi;
- axborotni himoya qilish vositalarini joriy etish, rivojlantirish, ulardan foydalanish ustidan nazoratni amalga oshiradi va ta'minlaydi, shuningdek qonun chiqaruvchi talablariga muvofiq axborot xavfsizligi sohasidagi faoliyatni sertifikatlash va litsenziyalashni amalga oshiradi;
- axborot aktivlarining xavfsizligi holatini vaqti-vaqti bilan baholaydi, axborot xavfsizligining amaldagi, davom etayotgan yoki ehtimoliy buzilishlarini aniqlaydi, hisobga oladi va ularga zudlik bilan javob qaytaradi.

3.3. Bankda axborot xavfsizligini ta'minlash bo'yicha vazifalarni amalga oshirish jarayonida amalga oshiriladigan aniq usullar va chora-tadbirlar ushbu Siyosatning 7-bo'limida keltirilgan.

4. HIMOYA OBYEKTLARI

4.1. Quyidagilar Bank axborot xavfsizligini himoya qilishning asosiy obyektlari hisoblanadi:

1) *Konfidensial ma'lumotlari* quyidagilar:

- tarqatish bo'yicha cheklangan xizmat (biznes) ma'lumotlari;
- bank, uning mijozlari, sheriklari va shartnoma munosabatlari ichidagi kontragentlarning tijorat sirini tashkil etuvchi 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*, shu jumladan Bank axborot bank tizimlarida amalga oshiriladigan axborot va to'lov jarayonlari.

3) *Xodimlar*:

- bank mijozlari va ular amalga oshiradigan operatsiyalar to'g'risida ma'lumot;

- bank xodimlari;

- Bank axborot tizimlari dasturiy ta'minot ishlab chiqaruvchilari.

4) *Bankning intellektual mulk obyektlari.*

5) *Ish stantsiyalari va boshqa so'nggi qurilmalar* (noutbuklar va planshetlar), serverlar, ma'lumotlarni saqlash (ma'lumotlarni saqlash tizimlari), ma'lumotlarni qayta ishlash va saqlashning boshqa vositalari.

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.

Bank foydalanishga ruxsat berilgan dasturiy ta'minot ro'yxatini yuritadi. Uni yuritish talablari, shuningdek dasturiy ta'minotni o'rnatish va undan foydalanish bilan bog'liq talablar *ushbu siyosatning 9-ilovasiga muvofiq* foydalanishga ruxsat berilgan dasturiy ta'minot ro'yxati bilan tartibga solinadi.

7) *Xizmatlar va axborot almashish tizimlari:*

- bankning barcha xodimlari uchun o'z pochta serveridan foydalangan holda tashkil etiladigan korporativ elektron pochta; bunda korporativ elektron pochta, shuningdek Internet tarmog'i bilan ishlash qoidalari Internet tarmog'i va korporativ elektron pochta bilan ishlash qoidalarida ushbu siyosatning 10 - ilovasiga muvofiq tartibga solinadi.

- elektron hujjat aylanish tizimi (EHAT) Myanor.uz;

- Bank xodimlari o‘rtasida tezkor xabar almashish uchun korporativ messenjer Anor Chat;

- IP telefoniya tizimi va Call-markaz;

- videokonferensaloqa tizimi.

8) *Jismoniy xavfsizlik tizimlari:*

- bankning xodimlari plastik identifikatsiya kartalari va biometrik ma'lumotlari (yuzni identifikatsiya qilish) asosida kirishni boshqarish va nazorat vositalaridan foydalangan holda Bosh ofis va IT-ofisning himoyalanadigan xonalariga kirishni nazorat qilishni ta'minlaydigan kirishni boshqarish va boshqarish tizimi Bosh ofis va IT-ofisda;

- Bosh ofis binolari, IT-ofis va bankomatlar perimetri bo‘ylab va ichkarisida o‘rnatilgan videokameralardan video kuzatuv va videoma’lumotlarni yig‘ish uchun videokuzatuv tizimi;

9) *Bank tarmoq infratuzilmasi* quyidagilarni tashkil etadi.

- Bankda boshqariladigan tarmoqni tashkil qilish uchun domen kontroller serveri (Bank asosiy ma'lumotlar qayta ishlash markazida joylashgan asosiy va yordamchi serverlar);

- korporativ tarmoqning asosiy kommutatorlari, Bank Bosh ofis, IT-ofis va

savdo ofisida lokal tarmoqlarga kirish kommutatorlari;

- Bosh ofisda, IT-ofisda va savdo ofislarida tashkil etilgan lokal tarmoqlar;
- korporativ tarmoqni tashkil qilish kanallari (Bosh ofis asosiy ma'lumotlarni qayta ishlash markazi), zahiraviy ma'lumotlarni qayta ishlash markazi, IT-ofis va savdo ofislari o'rtasidagi ulanishlar), shuningdek Bank korporativ tarmog'ini tashqi tarmoqlarga ulash uchun tashqi kanallar va O'zbekiston Respublikasi Markaziy bankining Internet va BTT;
- Bank asosiy ma'lumotlarni qayta ishlash markazi (Bosh ofis) va zaxira ma'lumotlarni qayta ishlash markazi ("O'zbektelekom" AK ATS-233 ma'lumotlar markazi) o'rtasida o'ziga tegishli optik tolali aloqa liniyalari ("qora" tolalar).

10) *Axborot resurslari:*

- Bank rasmiy sayti https://anorbank.uz/, asosan bankning ma'lumotlarni qayta ishlash markazida joylashgan
- Bankning asosiy ma'lumotlarni qayta ishlash markazida joylashgan BSS masofaviy bank tizimining Internet-banking veb-sayti.
- Bank tarkibiy bo'linmalari uchun bankning asosiy ma'lumotlarni qayta ishlash markazidagi serverda tashkil etilgan fayllarni saqlash;
- axborot tizimlarining ma'lumotlar bazalari, shu jumladan Bank ABT ma'lumotlar bazasi, ularning elektron arxivlari.

11) Himoyalangan axborotni tashuvchilar.

12) Himoyalangan xonalar: bankning Bosh ofisida konfidensial ma'lumotlar qayta ishlanadigan ofis xonalari, asosiy ma'lumotlarni qayta ishlash markazining server xonasi.

13) Axborot xavfsizligi vositalari (xavfsizlik devorlari, IDPS hujumlarini aniqlash va oldini olish vositalari, VPN vositalari, virusga qarshi himoya vositalari va boshqalar).

14) Bankning axborot tizimlari;

15) Nomoddiy aktivlar

4.2. Bankda quyidagi axborot tizimlari tashkil etilgan:

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

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

- ma'lumotlar bazasi serverlari (asosiy va zaxira ma'lumotlarni qayta ishlash markazlarida klaster rejimida ishlaydigan ikkita jismoniy ma'lumotlar bazasi serverlari);
- Bank korporativ tarmog'i orqali Bank bosh ofisi xodimlarining ABTga (ABT foydalanuvchilari) kirishi uchun server-ilovalar, ular asosiy ma'lumotlarni qayta ishlash markazidagi virtual serverlarda ularning zahira nusxasi ma'lumotlarni qayta ishlash markazida tashkil etilgan.

ABT foydalanuvchilari bank xodimlaridir.

2) BSS masofaviy bank tizimi (keyingi o'rinlarda BSS MBT tizimi deb yuritiladi) bu bankning yuridik mijozlariga raqamli bank xizmatlarini ko'rsatish uchun Internet-banking tizimi va bankning yuridik mijozlariga raqamli bank xizmatlarini ko'rsatish uchun mobil banking tizimi (mobil ilova) "Anor-bisness") va

jismoniy shaxslar ("Anorbank" mobil ilovasi).

BSS MBT tizimi ikkita virtual ma'lumotlar bazasi serverini va uchta virtual dastur serverini o'z ichiga oladi.

BSS MBT tizimining foydalanuvchilari mijozlar va bank xodimlaridir.

3) ELMA biznes-jarayonlarini boshqarish tizimi (keyingi o'rinlarda ELMA tizimi) bank mijozlariga xizmat ko'rsatish jarayonlarini avtomatlashtirish uchun (asosiy ma'lumotlarni qayta ishlash markazidagi virtual serverlar, ularning asosiy va zaxira ma'lumotlarni qayta ishlash markazlarida alohida jismoniy serverlarda zaxirasi bilan). Ushbu tizimning foydalanuvchilari bank xodimlaridir.

4) Bank mijozlarining kreditga layoqatliligi to'g'risidagi ma'lumotlarni yig'ish va qayta ishlash tizimi (qarz oluvchilarning kredit reytingi) Wings (keyingi o'rinlarda Wings tizimi deb yuritiladi), ikkita virtual ma'lumotlar bazasi serverlari va ikkita virtual dastur serverlaridan iborat bo'lib, ularning zaxira nusxasi ma'lumotlar markazida. Wings tizimining foydalanuvchilari bank xodimlaridir.

5) BillMaster hisob-kitob tizimi (keyingi o'rinlarda BillMaster tizimi deb yuritiladi), asosiy ma'lumotlarni qayta ishlash markazidagi virtual serverlardan iborat bo'lib, ular asosiy va zaxira ma'lumotlarni qayta ishlash markazlaridagi alohida jismoniy serverlarda bron qilinadi. BillMaster tizimining foydalanuvchilari bank xodimlaridir.

6) Billmaster o'zaro hisob – kitob tizimi (bundan buyon matnda BillMaster tizimi deb yuritiladi), asosan markaziy ma'lumotlar bazasining virtual serverlaridan iborat bo'lib, ularni asosiy va zaxira ma'lumotlar bazasining alohida jismoniy serverlarida zaxiralash mumkin. Tizim foydalanuvchilari bank xodimlari.

7) AGC (ADPMS – AGCning eski versiyasi) – bank xodimlarini qulay boshqarish, boshqarish va ulardan foydalanish uchun bankning barcha ma'lumotlar bazalarini bitta tizimga to'playdigan platforma. Tizim foydalanuvchilari bank xodimlari.

8) Anorhub – kirish boshqaruvchisi, shuningdek har bir murojaatning loglash funksiyasiga ega bo'lgan yagona markaz orqali bankning har qanday axborot tizimlari va axborot resurslariga qonuniy qo'ng'iroqlarni almashtirish. Tizim foydalanuvchilari bank xodimlari.

9) Qlik Sense-markazlashtirilgan saqlash va maxsus so'rovlar tili orqali real vaqtda ma'lumotlarni tahlil qilish va vizualizatsiya qilish platformasi. Tizim foydalanuvchilari bank xodimlari.

10) Confluence -yagona bilimlar bazasini yaratish maqsadida tashkilotlar tomonidan ichki foydalanish tizimi (texnik vazifalarni, shuningdek imtiyozlar jadvali loyihalari hujjatlarini, bankning ma'lum resurslaridan foydalanish algoritmini tuzish). Tizim foydalanuvchilari bank xodimlari.

11) Gitlab – o'z wiki, xatolarni kuzatish tizimi, CI/CD liniyasi va boshqa funksiyalarga ega bo'lgan GIT uchun bank kodi omborlarini boshqarish tizimi. Tizim foydalanuvchilari bank xodimlari.

12) Jira – IT mutaxassislari uchun loyihalarni rejalashtirish, taqsimlash, boshqarish va vazifalarni rejalashtirish platformasi bo'lib, u barcha jamoalar o'rtasida moslashuvchan hamkorlikni ta'minlaydi.

13) Keycloak - identifikatsiya va kirishni boshqarish bilan bitta tizimga kirishni ta'minlaydigan dasturiy mahsulot.

14) MerchantCabinet – Anorbank sheriklarining ishlashi uchun platforma (voqealarni kuzatish, sherikning hisob hisobotlarini tahlil qilish va chiqarish uchun).

15) ServiceDesk- IT xizmatlarini qo'llab-quvvatlash jarayonlarini tashkil qilish uchun platforma.

16) Verifix-savdo shoxobchalarida xodimlarning qatnashishini hisobga olish tizimi.

17) WEBIM-24/7 mobil ilova, Instagram va bot telegrammalarini qo'llab-quvvatlash botidan olingan barcha ma'lumotlarni call-markazlar xodimlari tomonidan tezkor javob berish uchun yagona tizimga to'plash uchun platforma.

18) Superset-markazlashtirilgan saqlash va maxsus so'rovlar tili orqali real vaqtda ma'lumotlarni tahlil qilish va vizualizatsiya qilish platformasi. Tizim foydalanuvchilari bank xodimlari.

19) 1C-bank biznesining barcha moliyaviy-xo'jalik faoliyatini qo'llab-quvvatlaydigan buxgalteriya hisobi va soliq hisobi tizimi.

4.3. Bank ABT barcha ichki axborot tizimlari, jumladan BSS masofaviy bank tizimi, ELMA, Wings va BillMaster tizimlari va boshqalar.

4.4 Bank ABT tashqi axborot tizimlari: O‘zbekiston Respublikasi Markaziy bankining bank axborot tizimlari, HUMO va UzCard protsessing tizimlari, Banklar assotsiatsiyasining Kredit byurosi tizimi va boshqa tashkilotlarning axborot tizimlari bilan o‘zaro hamkorlik qiladi (ma’lumotlar almashadi).

4.5. ABT xavfsiz IPSec VPN kanallarini tashkil etish bilan Markaziy bankning BTT orqali tashqi axborot tizimlari bilan o‘zaro aloqada bo‘ladi.

4.6. O‘zDSt 2814:2014 davlat standartiga muvofiq “Axborot texnologiyalari. Avtomatlashtirilgan tizimlar. Axborotga ruxsatsiz kirishdan himoyalanish darajasi bo‘yicha tasnifi” Bank ABT 3B xavfsizlik klassiga ega.

4.7. Bank axborot resurslarining xavfsizlik darajasi bo‘yicha tasnifi mazkur Siyosatning 11-ilovasiga muvofiq Bank Axborot resurslari reestrida keltirilgan.

4.8. 1-jadvalda ko'rsatilgan Bank axborot tizimlarining ma'lumotlar bazalarida bank xodimlari va bank mijozlarining shaxsiy ma'lumotlari mavjud. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2022-yil 5-oktabrdagi “Shaxsiy ma’lumotlarni qayta ishlash sohasidagi ayrim me’yoriy-huquqiy hujjatlarni tasdiqlash to‘g‘risida”gi 570-son qaroriga muvofiq mazkur ma’lumotlar bazalariga tegishli himoya darajasi belgilangan. .

Bank axborot tizimlarida qayta ishlangan shaxsiy ma’lumotlarni himoya qilishga qo‘yiladigan talablar Bank Boshqaruvining 2023-yil 16-maydagi 7-1 bayonnomasi bilan tasdiqlangan “Anor Bank” AJ xodimlarining shaxsiy ma’lumotlariga ishlov berish to‘g‘risidagi nizomda belgilangan..

1-jadval. Belgilangan himoya darajasiga ega bo'lgan bankning shaxsiy ma'lumotlarini qayta ishlash uchun ma'lumotlar bazalari ro'yxati

Ma'lumotlar bazasi nomi	Shaxsiy ma'lumotlar turi	Himoya darajasi
ABT ma'lumotlar bazasi	Bank mijozining shaxsiy ma'lumotlari	2 darajasi
RBS BSS tizimi ma'lumotlar bazasi		2 darajasi
Wings tizimi ma'lumotlar bazasi		2 darajasi
BillMaster tizimi ma'lumotlar bazasi		2 darajasi
KeyCloak tizimi ma'lumotlar bazasi		2 darajasi
Oktell tizimi ma'lumotlar bazasi		2 darajasi
SKUD ma'lumotlar bazasi	Bank xodimlarining shaxsiy ma'lumotlari	1 darajasi

4.9 Bank himoya qilish obyektlari ushbu Siyosatning 18-ilovasida ko‘rsatilgan apparat-dasturiy ta’minot vositalaridan foydalangan holda tashkil etiladi.

5. AXBOROT XAVFSIZLIGI RISK VA TAHDIDLARNING MODELI

5.1. Bank axborot xavfsizligiga tahdid modeli ushbu Siyosatning 4-bobida ko‘rsatilgan har bir muhim va muhim himoya obyekti uchun aniqlanadi va quyidagilarni o‘z ichiga oladi:

- himoyalangan obyektning tavsifi;
- himoyalangan obyektga xavfsizlikga mumkin bo'lgan tahdidlarining ro'yxati va tavsifi;
- buzg'unchi modeli;
- mumkin bo'lgan zaifliklar;
- tahdidlarni amalga oshirish usuli;
- tahdidlarni amalga oshirish oqibatlari.

5.2. Bankning axborot xavfsizligiga tahdidlar paydo bo'lish xususiyatiga ko'ra tabiiy (obyektiv) va sun'iy (subyektiv) bo'lishi mumkin.

5.3. Axborot xavfsizligiga tahdidlarning manbalari ichki (tahdidlar manbai Bank ichida) va tashqi (tahdidlar manbai Bankdan tashqarida) bo'lishi mumkin.

5.4. Axborot xavfsizligiga tahdidlar qasddan (aniq maqsadga erishish uchun qasddan) va tasodifiy (uskunalar, dasturiy ta'minot va xodimlardagi xatolar natijasida yuzaga keladi) bo'lishi mumkin.

5.5. Bankning axborot xavfsizligiga asosiy tahdidlar modeli 2-jadvalda keltirilgan.

5.6. Axborot xavfsizligi darajasini aniqlash maqsadida Bank risklarni tahlil qilish va baholashni amalga oshiradi. Hujumlar axborot xavfsizligiga tahdidlar sodir bo'lgan taqdirda zarar va yo'qotish ehtimoli bilan belgilanadi. Risklar himoya qilinadigan obyektga haqiqiy ta'sir qilish xavfi mavjudligi sababli yuzaga keladi.

2-jadval. KDB Bankning axborot xavfsizligiga asosiy tahdidlar modeli

Turkumi	T/r	Tahdid nomi	Manbaining ko‘rinishi, tabiati va sababi*	Ta'sir qilish obyektlari va oqibatlari
Jismoniy tahdidlar	TP01	Yong‘in	A, D, E, F, B, C	Barcha himoya obyektlari. Muvaffaqiyatsizlik yoki yo‘qotish
	TP02	Suv toshishi	A, D, E, F, B, C	
	TP03	Ifloslanish, zararli radiatsiya	A, D, E, F, B, C	
	TP04	Katta baxtsiz hodisa	A, D, E, F, B, C	
	TP05	Portlash, halokat	A, D, E, F, B, C	
	TP06	Chang, korroziya, muzlash	A, D, E, F, B, C	
Tabiiy tahdidlar	TN01	Iqlim hodisasi	A, E, C	Barcha himoya obyektlari. Muvaffaqiyatsizlik yoki yo‘qotish
	TN02	Seysmik hodisa	A, E, C	
	TN03	Vulqon hodisasi	A, E, C	
	TN04	Meteorologik hodisa	A, E, C	
	TN05	Suv toshqini	A, E, C	
	TN06	Pandemiya/epidemiya hodisasi	A, E, C	
Infratuzilmaning ishlamay qolishi	TI01	Ta'minot tizimining ishdan chiqishi	A, D, F, C	Uskuna va dasturiy ta'minot, ish stantsiyalari va serverlari, mahalliy tarmoq, korporativ elektron pochta, axborot tizimlari va resurslari. Muvaffaqiyatsizlik, ishning to‘xtatilishi
	TI02	Sovutish yoki shamollatish tizimining ishlamay qolishi	A, D, F, B, C	
	TI03	Energiya ta'minotining buzilishi	A, D, E, F, C	
	TI04	Telekommunikatsiya tarmog‘ining ishdan chiqishi	A, D, E, F, C	
	TI05	Telekommunikatsiya uskunalari ishlamay qolishi	A, D, F, B	
	TI06	ElektromagnAT nurlanish	A, D, E, F, C	
	TI07	Termal nurlanish	A, D, E, F, B, C	
	TI08	ElektromagnAT impulslar	A, D, E, F, C	
Texnik muvaffaqiyatsizliklar	TT01	Qurilma yoki tizimning ishdan chiqishi	A, F, B	Uskuna va dasturiy ta'minot, ish stantsiyalari va serverlari, mahalliy tarmoq, korporativ elektron pochta, axborot tizimlari va resurslari. Muvaffaqiyatsizlik, ishning uzilishi,
	TT02	Axborot tizimining to‘yinganligi	A, D, F, B	
	TT03	Axborot tizimini ta`mirlash qobiliyatini buzilishi	A, D, F, B	

				uskuna yoki ma'lumotlarning yo‘qolishi
Xodimlar xarakati	TH01	Terrorizm, hujumlar, sabotaj	D, F, B, C	Barcha himoya obyektlari. Muvaffaqiyatsizlik yoki yo‘qotish
	TH02	Ijtimoiy muhandislik	D, F, B, C	Tarmoqlar va axborot tizimlarining apparat va dasturiy ta'minoti. Maxfiylik, yaxlATlik va mavjudlikni buzish
	TH03	Qurilmaning nurlanishini ushlab turish	D, F, B, C	Axborot, konfidensiallikni buzish
	TH04	Masofaviy monATоring	D, F, B, C	
	TH05	Tinglash	D, F, B, C	
	TH06	Ommaviy axborot vositalari yoki hujjatlarni o‘g‘irlash	D, F, B, C	Axborot tashuvchi va saqlovchi vositalar va hujjatlar. YaxlATlik va konfidensiallikni buzish
	TH07	Uskunani o‘g‘irlash	D F, B, C	Uskunalar. Yo‘qotish, faoliyatni olib borishning buzilishi
	TH08	Raqamli identifikatorni yoki identifikatsiya ma'lumotlarini o‘g‘irlash	D, F, B, C	Ish stantsiyalari, serverlar, tarmoqlar va axborot tizimlari. Ruxsatsiz kirish
	TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma`lumot tashuvchi qurilmalardan ma`lumot olish	D, F, B, C	Axborot, konfidensiallikni buzish
	TH10	Axborotni oshkor qilish	A, D, F, B, C	
	TH11	Ishonchsiz manbalardan ma'lumotlarni kirATish	A, D, F, B, C	Axborot, ishonchlilikning buzilishi
	TH12	Uskunani buzish	D, F, B, C	Uskuna va ma'lumot. Funktsionallik, yaxlATlik, konfidenaiallik va mavjudlikni buzish

	TH13	Dasturiy ta'minotni buzish	A, D, F, B, C	Dasturiy ta'minot vositalari va ma'lumotlar. Funktsionallik, yaxlATlik, konfidenaiallik va mavjudlikni buzish
	TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	D, F, B, C	Axborot resurslari va tizimlari. Ruxsatsiz kirish
	TH15	Takroriy hujum, o‘rtadagi odam hujumi	D, F, B, C	Ma `lumot. Ruxsatsiz kirish
	TH16	Shaxsiy ma'lumotlarni ruxsatsiz qayta ishlash	A, D, F, B, C	
	TH17	Obyektlarga ruxsatsiz kirish	D, F, B, C	Barcha himoya obyektlari. Ruxsatsiz kirish
	TH18	Qurilmalardan ruxsatsiz foydalanish	D, F, B, C	Qurilma. Nosozlik, ish faoliyatining to‘xtashi
	TH19	Qurilmalardan noto‘g‘ri foydalanish	A, D, F, B, C	
	TH20	Qurilmalar yoki ma`lumot tashuvchilarni shikastlash	A, D, F, B, C	Qurilma. Axborotlarni tashuvchi va saqlovchi vositalar Nosozlik, ish faoliyatining to‘xtashi
	TH21	Soxta dasturiy ta'minotni nusxalash	D, F, B, C	Dasturiy ta'minot, Funktsionallik va mualliflikning buzilishi
	TH22	Qalbaki yoki nusxalangan dasturiy ta`minotdan foydalanish	A, D, F, B, C	
	TH23	Ma`lumotlarga shikast yetkazish	D, F, B, C	Ma'lumotlar yaxlATligini buzish
	TH24	Noqonuniy ma'lumotlarni qayta ishlash	D, F, B, C	Ma'lumotlar, ma'lumotlardan noqonuniy foydalanish, mualliflik huquqining buzilishi
	TH25	Zararli dasturlarni yuborish yoki tarqatish	A, D, E, F, B, C	Ish stantsiyalari, tarmoq, axborot tizimlari va resurslari. Nosozlik, nosozlik, yo‘qotish, ruxsatsiz kirish

	TH26	Joylashuvni aniqlash	D, F, B, C	Axborot, konfidensiallikni buzish
Xizmatlar yoki funksiyalarni buzish	TC01	Foydalanishda xatoliklar	A, F, B, C	Uskuna va dasturiy ta'minot, tarmoq, axborot tizimlari va resurslari, axborot. Nosozlik, nosozlik, yo‘qotish, ruxsatsiz kirish
	TC02	Huquqlar yoki ruxsatlarni suiiste'mol qilish	A, D, F, B, C	
	TC03	Huquqlar yoki ruxsatlarni soxtalashtirish	D, F, B, C	
	TC04	Harakatlarni rad etish	D, F, B, C	
Tashkiliy tahdidlar	TO01	Xodimlarning etishmasligi	A, E, F, B	Uskuna va dasturiy ta'minot, tarmoq, axborot tizimlari va resurslari, axborot. Ish faoliyatining buzilishi
	TO02	Resurslarning etishmasligi	A, E, F, B	
	TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	A, E, F, C	
	TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	A, D, F, B, C	
Saqlash tizimlari va infratuzilmasiga tahdidlar	TD01	Ruxsat etilmagan foydalanish	D, F, B, C	Saqlash tizimi va infratuzilmasi, saqlash joylaridagi ma'lumotlar, Axborot tashuvchi yoki saqlovchi vositalar Axborotning yaxlATligi, mavjudligi va maxfiyligini buzish
	TD02	Ruxsatsiz kirish	D, F, B, C	
	TD03	Qonunlar va me'yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	A, D, F, B, C	
	TD04	Saqlash tizimlariga DoS va DDoS hujumlar	D, F, C	
	TD05	Ma'lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	A, D, F, B, C	
	TD06	Ma'lumotlar sizib chiqishi	D, F, B	
	TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy yo‘qotish	A, D, F, B, C	
	TD08	Zararli dastur hujumi yoki inyeksiyasi	D, F, B, C	
	TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	A, D, F, B	

* Izoh: tahdidlar quyidagi mezonlarga ko‘ra tasniflanishi mumkin:
- vujudga kelish manbasiga ko‘ra: B-ichki, C-tashqi;
- vujudga kelishi sababli: A-tasodifiy, D-qasddan;
- vujudga kelish xususiyatiga ko‘ra: E – tabiiy yoki obyektiv, F – subyektiv.

5.7. Bankda risklarni identifikatsiyalash axborot xavfsizligi risklarini aniqlash, tahlil qilish va baholashni O‘zMSt ISO/IEC 27005:2024 “Axborot xavfsizligi, kiberxavfsizlik va konfidensiallikni muhofaza qilish. Axborot xavfsizligi xavflarini boshqarish bo’yicha qo’llanma”.

5.8. Risklarni identifikatsiyalash natijalari qo‘llanma bo‘lib xizmat qiladi, tegishli boshqaruv harakatlarini va axborot xavfsizligini boshqarishning ustuvor yo‘nalishlarini belgilaydi, shuningdek ushbu xavflardan himoya qilish uchun tanlangan chora-tadbirlar, usullar va vositalarni amalga oshirishga qaratilgan bo‘lishi kerak.

5.9. Risklarni identifikatsiyalash risklarni baholashga tizimli yondashuvni (riskni tahlil qilish) va xavflarning ahamiyatini aniqlash uchun baholangan risklarni xavf mezonlari bilan taqqoslashni o‘z ichiga oladi.

Risklarni aniqlashdan tashqari, risklarni boshqarish jarayoni quyidagilarni o'z ichiga olishi kerak: riskni davolash, riskni qabul qilish, xavf bilan bog'lanish va maslahatlar, risklarni monitoring qilish va tahlil qilish.

5.10. Axborot xavfsizligi bo'yicha xavflarni aniqlash Axborot xavfsizligi boshqarmasi tomonidan amalga oshiriladi.

5.11. Risklarni baholash metodologiyasi, shuningdek, Bank himoyasining asosiy obyektlariga nisbatan axborot xavfsizligi risklarini hisoblash ushbu Siyosatning 17-ilovasida keltirilgan.

5.12. Axborot xavfsizligi tavakkalchiligini baholash natijalari risklarni qabul qilish mezonlari bilan taqqoslanadi, bu qiymatdan oshib ketgan risklar qabul qilinishi mumkin emas deb hisoblanadi. Axborot xavfsizligi risklarini qabul qilish mezonlari 3-jadvalda keltirilgan.

3-jadval. KDB bank axborot xavfsizligi risklarini qabul qilish mezonlari

Xavf darajasi	Xavfni baholash	Miqdorni aniqlash	Tavsifi
Past (yashil)	Qanday bo‘lsa shundayligicha qabul qilinadi	0-1	Xavf boshqa harakatlarsiz qabul qilinishi mumkin
O‘rta (sariq)	Boshqaruv vositalari mavjud bo‘lgan hollarda qabul qilinadi	1-2	O‘rta va uzoq muddatli istiqbolda doimiy takomillashtirish doirasida risklarni boshqarish faoliyati va ichidagi harakatlarni belgilash chora-tadbirlarini o‘tkazish lozim
Yuqori (qizil)	Qabul qilib bo‘lmaydigan	2 dan yuqori	Qisqa muddatda xavfni kamaytirish choralarini ko‘rish kerak.

5.13. Bankning asosiy himoya obyektlariga nisbatan axborot xavfsizligi risklarini baholash natijalari ularni risklarni qabul qilish mezonlari bilan taqqoslagandan so'ng rangli kodlangan matritsa shaklida taqdim etiladi va 4-jadvalda keltirilgan.

5.14. “Yuqori” (qizil rangdagi) qiymatiga ega bo'lgan axborot xavfsizligi xavfi ularning qiymati riskni qabul qilish mezonlaridan oshib ketishini anglatadi va ularga nisbatan ushbu risklarni kamaytirish choralarini ko'rish kerak. Ushbu chora-

tadbirlar tahdidning paydo bo'lishini kamaytirish yoki yo'q qilishga yoki zaiflik darajasini yo'q qilishga yoki kamaytirishga qaratilgan bo'lishi mumkin.

5.15. Agar choralar ko'rilsa, risklar xavf parametrlarining yangi qiymatlarini va zaiflikning mavjudligini hisobga olgan holda qayta hisoblab chiqiladi. Olingan yangi xavf qiymati qoldiq riskdir.

"Yuqori" darajadagi axborot xavfsizligi riskni kamaytirish choralari, shuningdek choralar ko'rilgandan keyin axborot xavfsizligining qoldiq xavfi 5-jadvalda keltirilgan.

5.16. Shuningdek, "yuqori" darajadagi axborot xavfsizligi riskni kamaytirish uchun tegishli xususiyatlarga ega bo'lgan zarur ma'lumotlarni himoya qilish vositalarini tanlash kerak. KDB bankda qo'llaniladigan axborotni himoya qilish vositalariga qo'yiladigan talablar ushbu siyosatning 7-bo'limida keltirilgan.

4 - Jadval. Bankning himoya obyektlariga nisbatan axborot xavfsizligi risklarini baholash natijalari

№	Tahdidning tavsifi	ABT	RBS BSS tizimi	ELMA, CRM, AGC (ADPMS) va Anorhub (MercantCabinet) tizimlari	Tizimlar Bill Master, EDMS Myanor, Superset, 1C	Systems Wings, Qlik Sense, WEBIM, KeyCloak	Jira, ServiceDesk, Verifix, Oktell tizimlar	Confluence, Gitlab tizimlar	Korporativ electron pochta	IP telefoniya tizimi va Call markazi	Server domen boshqaruvchisi	Fayl server	Rasmiy veb sayt	Ishchi so'nggi qurilmalar	SKUD	Video kuzatuv tizimi
TP01	Yong'in	0,59	0,59	0,52	0,46	0,39	0,33	0,26	0,46	0,39	0,46	0,46	0,28	0,54	0,30	0,26
TP02	Suv toshishi	0,47	0,47	0,42	0,37	0,32	0,26	0,21	0,37	0,32	0,37	0,37	0,23	0,44	0,26	0,23
TP03	Ifloslanish, zararli radiatsiya	0,18	0,18	0,16	0,14	0,12	0,10	0,08	0,14	0,12	0,14	0,14	0,10	0,18	0,14	0,12
TP04	Katta baxtsiz hodisa	0,66	0,66	0,58	0,51	0,44	0,36	0,29	0,51	0,44	0,51	0,51	0,33	0,59	0,48	0,41
TP05	Portlash, halokat	0,23	0,23	0,21	0,18	0,15	0,13	0,10	0,18	0,15	0,18	0,18	0,11	0,23	0,24	0,21
TP06	Chang, korroziya, muzlash	0,23	0,23	0,21	0,18	0,15	0,13	0,10	0,18	0,15	0,18	0,18	0,11	0,21	0,17	0,15
TN01	Iqlim hodisasi	0,90	0,90	0,80	0,70	0,60	0,50	0,40	0,70	0,60	0,70	0,70	0,48	0,96	0,35	0,30
TN02	Seysmik hodisa	0,68	0,68	0,60	0,53	0,45	0,38	0,30	0,53	0,45	0,53	0,53	0,50	1,05	0,53	0,45
TN03	Vulqon hodisasi	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
TN04	Meteorologik hodisa	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,32	0,64	0,28	0,24
TN05	Suv toshqini	0,84	0,84	0,75	0,65	0,56	0,47	0,37	0,65	0,56	0,65	0,65	0,37	0,80	0,65	0,56
TN06	Pandemiya/epidemiya hodisasi	0,54	0,54	0,48	0,42	0,36	0,30	0,24	0,42	0,36	0,42	0,42	0,40	0,84	0,42	0,36
TI01	Ta'minot tizimining ishdan chiqishi	1,26	1,26	1,12	0,98	0,84	0,70	0,56	0,98	0,72	1,12	1,12	0,64	1,32	1,12	0,96
TI02	Sovutish yoki shamollatish tizimining	1,58	1,58	1,40	1,23	1,12	0,93	0,75	1,39	1,12	1,47	1,55	0,84	1,75	1,47	1,26
TI03	Energiya ta'minotining buzilishi	1,80	1,80	1,60	1,40	1,28	1,07	0,85	1,59	1,36	1,59	1,68	0,91	1,88	1,47	1,26
TI04	Telekommunikatsiya tarmog'ining	1,89	1,89	1,68	1,47	1,32	1,10	0,88	1,61	1,44	1,68	1,61	0,72	1,68	1,61	1,38

TI05	Telekommunikatsiya uskunalari	1,62	1,68	1,49	1,31	1,16	0,97	0,77	1,40	1,20	1,49	1,49	0,88	1,80	1,45	1,24
TI06	ElektromagnAT nurlanish	0,54	0,54	0,48	0,42	0,36	0,30	0,24	0,42	0,36	0,42	0,42	0,24	0,48	0,21	0,18
TI07	Termal nurlanish	0,72	0,72	0,64	0,56	0,48	0,40	0,32	0,56	0,48	0,56	0,56	0,32	0,48	0,56	0,48
TI08	ElektromagnAT impulslar	0,54	0,54	0,48	0,42	0,36	0,30	0,24	0,42	0,36	0,42	0,42	0,24	0,48	0,14	0,12
TT01	Qurilma yoki tizimning ishdan chiqishi	3,40	3,35	2,98	2,61	1,81	1,84	1,47	2,58	2,22	1,96	2,53	1,42	1,90	1,98	1,80
TT02	Axborot tizimining to‘yinganligi	1,35	1,35	1,20	1,05	0,90	0,75	0,60	1,05	0,90	1,05	1,05	0,72	1,38	0,84	0,72
TT03	Axborot tizimini ta`mirlash qobiliyatini buzilishi	0,92	0,92	0,81	0,71	0,63	0,53	0,42	0,76	0,63	0,79	0,81	0,48	0,89	0,76	0,65
TH01	Terrorizm, hujumlar, sabotaj	0,37	0,38	0,34	0,30	0,26	0,22	0,18	0,35	0,27	0,33	0,31	0,21	0,38	0,29	0,25
TH02	Ijtimoiy muhandislik	1,26	1,32	1,17	1,02	0,92	0,76	0,61	1,25	0,95	1,16	1,07	0,79	1,34	0,98	0,84
TH03	Qurilmaning nurlanishini ushlab turish	0,81	0,81	0,72	0,63	0,54	0,45	0,36	0,63	0,54	0,63	0,63	0,36	0,72	0,63	0,54
TH04	Masofaviy monATоring	0,70	0,70	0,62	0,55	0,50	0,42	0,34	0,59	0,50	0,63	0,59	0,38	0,68	0,59	0,50
TH05	Tinglash	0,86	0,86	0,77	0,67	0,65	0,54	0,43	0,76	0,65	0,84	0,76	0,53	1,08	0,76	0,65
TH06	Ommaviy axborot vositalari yoki hujjatlarni o‘g‘irlash	1,37	1,37	1,22	1,06	0,94	0,78	0,62	1,09	0,94	1,12	1,09	0,72	1,42	1,06	0,91
TH07	Uskunani o‘g‘irlash	0,83	0,83	0,74	0,64	0,58	0,48	0,38	0,67	0,58	0,70	0,67	0,46	0,84	0,67	0,58
TH08	Raqamli identifikatorni yoki	1,27	1,27	1,13	0,99	0,87	0,73	0,58	1,02	0,87	1,05	1,02	0,69	1,21	1,02	0,87
TH09	Tashlab yuborilgan yoki takror ishlatilayotgan ma`lumot tashuvchi qurilmalardan ma`lumot olish	1,44	1,44	1,28	1,12	1,02	0,85	0,68	1,19	1,02	1,26	1,19	0,84	1,44	1,12	0,96
TH10	Axborotni oshkor qilish	2,15	2,09	2,07	1,31	1,17	0,98	0,78	1,37	1,17	1,42	1,37	0,81	1,35	1,37	1,17
TH11	Ishonchsiz manbalardan ma'lumotlarni kirATish	1,65	1,73	1,53	1,34	1,20	1,00	0,80	1,40	1,20	1,46	1,40	0,83	1,35	1,28	1,10
TH12	Uskunani buzish	0,86	0,86	0,77	0,67	0,58	0,48	0,38	0,67	0,58	0,67	0,67	0,40	0,72	0,64	0,55
TH13	Dasturiy ta'minotni buzish	1,14	1,16	1,04	0,91	0,79	0,66	0,53	0,91	0,78	0,91	0,93	0,59	1,01	0,76	0,65
TH14	Veb-aloqa orqali Drive-by ekspluatatsiyasidan foydalanish	1,03	1,13	1,00	0,88	0,79	0,65	0,52	1,07	0,82	0,99	0,92	0,63	1,18	0,57	0,49

TH15	Takroriy hujum, o‘rtadagi odam hujumi	1,08	1,14	1,01	0,89	0,80	0,67	0,53	1,12	0,80	0,98	0,93	0,67	1,04	0,79	0,68
TH16	Shaxsiy ma'lumotlarni ruxsatsiz qayta ishlash	1,64	1,67	1,48	1,30	1,11	0,93	0,74	1,30	1,13	1,32	1,30	0,86	1,53	1,22	1,05
TH17	Obyektlarga ruxsatsiz kirish	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,27	0,64	0,37	0,32
TH18	Qurilmalardan ruxsatsiz foydalanish	0,82	0,82	0,73	0,64	0,55	0,46	0,37	0,64	0,55	0,64	0,64	0,41	0,75	0,64	0,55
TH19	Qurilmalardan noto‘g‘ri foydalanish	1,08	1,08	0,96	0,84	0,72	0,60	0,48	0,84	0,72	0,84	0,84	0,48	0,72	0,84	0,72
TH20	Qurilmalar yoki ma`lumot tashuvchilarni shikastlash	0,99	0,99	0,88	0,77	0,72	0,60	0,48	0,77	0,66	0,77	0,84	0,60	1,20	0,63	0,54
TH21	Soxta dasturiy ta'minotni nusxalash	1,50	1,50	1,33	1,16	1,00	0,83	0,67	1,16	1,00	1,16	1,16	0,74	1,42	1,04	0,89
TH22	Qalbaki yoki nusxalangan dasturiy ta`minotdan foydalanish	0,96	0,96	0,85	0,75	0,68	0,57	0,45	0,79	0,68	0,84	0,79	0,51	0,88	0,70	0,60
TH23	Ma`lumotlarga shikast yetkazish	1,13	1,13	1,00	0,88	0,75	0,63	0,50	0,88	0,75	0,88	0,88	0,54	1,32	0,88	0,75
TH24	Noqonuniy ma'lumotlarni qayta ishlash	1,49	1,53	1,36	1,19	1,02	0,85	0,68	1,19	1,02	1,19	1,19	0,72	1,20	1,12	0,96
TH25	Zararli dasturlarni yuborish yoki tarqatish	1,14	1,20	1,07	0,93	0,84	0,70	0,56	1,17	0,84	1,03	0,98	0,64	1,04	0,70	0,60
TH26	Joylashuvni aniqlash	0,45	0,45	0,40	0,35	0,30	0,25	0,20	0,35	0,36	0,42	0,35	0,24	0,42	0,35	0,30
TC01	Foydalanishda xatoliklar	1,18	1,18	1,05	0,92	0,83	0,69	0,55	0,94	0,81	0,96	0,96	0,60	1,11	0,79	0,68
TC02	Huquqlar yoki ruxsatlarni suiiste'mol qilish	1,49	1,49	1,32	1,16	0,99	0,83	0,66	1,16	0,99	1,16	1,16	0,66	1,08	1,16	0,99
TC03	Huquqlar yoki ruxsatlarni	1,20	1,20	1,07	0,93	0,84	0,70	0,56	0,98	0,84	1,03	0,98	0,67	1,04	0,98	0,84
TC04	Harakatlarni rad etish	1,41	1,41	1,26	1,10	0,94	0,79	0,63	1,10	0,94	1,10	1,10	0,63	1,11	1,54	1,32
TO01	Xodimlarning etishmasligi	1,26	1,26	1,12	0,98	0,84	0,70	0,56	0,98	0,84	0,98	0,98	0,56	0,84	0,98	0,84
TO02	Resurslarning etishmasligi	1,44	1,44	1,28	1,12	1,08	0,90	0,72	1,40	1,20	1,40	1,40	0,64	1,44	1,40	1,20
TO03	Xizmat ko‘rsatuvchining to‘lovga layoqatsizligi	1,26	1,26	1,12	0,98	0,84	0,70	0,56	0,98	0,72	1,12	1,12	0,64	1,32	1,12	0,96

TO04	Qonunchilik yoki normativ-huquqiy hujjatlarning buzilishi	1,54	1,54	1,37	1,20	1,08	0,94	0,75	1,32	1,08	1,38	1,26	0,79	1,44	1,26	1,08
TD01	Ruxsat etilmagan foydalanish	1,23	1,25	1,11	0,97	0,83	0,70	0,56	0,97	0,85	0,99	0,97	0,64	1,15	0,92	0,79
TD02	Ruxsatsiz kirish	0,48	0,48	0,43	0,37	0,32	0,27	0,21	0,37	0,32	0,37	0,37	0,27	0,64	0,37	0,32
TD03	Qonunlar va me'yoriy hujjatlarga rioya qilmaslik uchun yuridik javobgarlik	1,54	1,54	1,37	1,20	1,08	0,94	0,75	1,32	1,08	1,38	1,26	0,79	1,44	1,26	1,08
TD04	Saqlash tizimlariga DoS va DDoS	1,89	1,89	1,68	1,47	1,26	1,05	0,84	1,47	1,26	1,47	1,47	0,84	1,26	1,26	1,08
TD05	Ma'lumotlarga zarar etkazish, o‘zgartirish va yo‘q qilish	1,40	1,40	1,25	1,09	0,96	0,80	0,64	1,12	0,96	1,15	1,12	0,75	1,37	1,09	0,94
TD06	Ma'lumotlar sizib chiqishi	2,09	2,09	1,50	1,31	1,17	0,98	0,78	1,37	1,17	1,42	1,37	0,81	1,35	1,37	1,17
TD07	Axborot tashuvchi yoki saqlovchi vositani o‘g‘irlash yoki tasodifiy	0,79	0,79	0,70	0,62	0,58	0,48	0,38	0,62	0,53	0,62	0,67	0,48	0,96	0,50	0,43
TD08	Zararli dastur hujumi yoki inyeksiyasi	1,14	1,20	1,07	0,93	0,84	0,70	0,56	1,17	0,84	1,03	0,98	0,64	1,08	0,70	0,60
TD09	Noto‘g‘ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	2,13	2,13	2,04	1,84	1,22	1,02	0,82	1,43	1,22	1,51	1,43	1,01	1,73	1,34	1,15

5-jadval. Axborot xavfsizligi xavfini kamaytirish bo'yicha chora-tadbirlar, shuningdek chora-tadbirlar ko'rilganidan keyin qoldiq axborot xavfsizligi xavfi

Tahdidning nomlanishi	**Riskning bahosi**	**Himoya obyektlari**	**Rejalashtirilgan chora-tadbirlar**	**Qolgan risk**
Qurilma yoki tizimning ishlamay qolishi	3,40	ABT	1.Konfiguratsiya, sozlamalar va dasturiy ta'minotdagi o'zgarishlarni nazorat qilish va hisobga olish 2. Dasturiy ta'minotni ishga tushirishdan oldin tekshirish jarayonlarini tartibga solish va amalga oshirish, dasturni kiritishdan oldin sinovdan o'tkazish (sinov operatsiyasi)	1,5
	3,35	RBS tizimi BSS		1,44
	2,98	ELMA, CRM, AGC (ADPMS) va Anorhub (MercantCabinet) tizimlari		1,35

	2,61	Tizimlar Bill Master, EDMS Myanor, Superset, 1C	3. Dasturiy ta'minotga o'zgartirishlar kiritish tartibini aniqlash va amalga oshirish 4.O'rnatish vositalarini hisobga olish 5.Dasturiy ta'minotni yangilash va o'zgartirishlarni hisobga olish 6. Tabiiy ofatlarni tiklash rejalariga ega bo'lish va o'qitish. 7. Davriy ta'mirlash ishlarini bajarish.	1,2
	2,58	Korporativ elektron pochta		1,18
	2,22	IP telefoniya tizimi va qo'ng'iroqlar markazi		0,95
	2,53	Fayl serveri		1,13
Axborotni oshkor qilish qilish	2,15	ABT	1. Foydalanuvchilar va administratorlarning majburiyatlarini hujjatlashtirish. 2. Foydalanuvchilarga mas'uliyatni yetkazish bo'yicha trening o'tkazish 3.Huquqbuzarliklar uchun javobgarlikni oshirish, huquqbuzarlarga nisbatan choralar ishlab chiqish va ularni qo'llash 4.DLP agentlarini barcha xodimlarning ish stantsiyalariga o'rnatish	1,7
	2,09	RBS BSS tizimi		1,56
	2,07	ELMA, CRM, AGC (ADPMS) va Anorhub (MercantCabinet) tizimlari		1,02
Ma'lumotlar sizib chiqishi	2,09	ABT	1. Barcha xodimlarning ish stantsiyalarida DLP agentlarini o'rnatish 2. Imtiyozli foydalanuvchilarning ma'lumotlar omboriga kirish huquqini olish va ularni boshqarish tartibini tartibga solish. 3. Axborot resurslarini himoyalangan axborot darajasiga qarab tasniflash 4. Himoyalangan axborot vositalarini hisobga olish	0,98
	2,09	RBS BSS tizimi		0,98
Noto'g'ri ishlov berish yoki foydalanish tugagandan keyin utilizatsiya qilish	2,13	ABT	1. Uskunalar va axborot tashuvchi vositalarini hisobdan chiqarish, yo'q qilish va utilizatsiya qilish tartibini tartibga solish va ularga rioya qilish 2.Masul shaxslarni tayinlash 3.Axborot vositalaridagi qoldiqlarni qayta ishlash va yo'q qilishning samarali usullaridan foydalanish 4. Qayta ishlanadigan axborot tashuvchi vositalarini to'g'ri saqlashni ta'minlash 5. Utilizatsiya qilish tartib-qoidalarining bajarilishini nazorat qilish	1,25
	2,13	Internet-banking va mobil banking tizimlari		1,25
	2,04	BPM, CRM tizimlari, Karaf va Artemis ma'lumotlar shinasi		0,98

6. AXBOROT XAVFSIZLIGI BUZG‘UNCHISI MODELI

6.1. 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.

6.2. Bankning himoya obyektlariga nisbatan huquqbuzarlar uning xodimlari, ham himoya qilish obyektlariga bevosita (jismoniy va/yoki mantiqiy) kirish huquqiga ega bo‘lganlar ham, unga ega bo‘lmaganlar ham bo‘lishi mumkin. Shuningdek, bank xodimlari bo'lmagan shaxslar.

6.3. Bankda potentsial qoidabuzarlarni aniqlash va ularning bankning himoyalangan obyektlariga axborot xavfsizligi tahdidlarini amalga oshirish nuqtai nazaridan amaliy va nazariy imkoniyatlarini baholash maqsadida axborot xavfsizligini buzuvchi modeli ishlab chiqiladi.

6.4. Bankning axborot xavfsizligini buzuvchilar ichki bo'lishi mumkin, ularga quyidagilar kiradi:

1) axborot tizimlari va tarmoqlaridan ro‘yxatdan o‘tgan (vakolatli) foydalanuvchi (to‘g‘ridan-to‘g‘ri foydalanuvchi) bo‘lgan bank xodimlari;

2) axborot tizimlari va tarmoqlaridan foydalanuvchi bo‘lmagan bank xodimlari (xona va binolarga xizmat ko‘rsatuvchi texnik xodimlar va boshqalar);

3) bankning texnik vositalariga xizmat ko'rsatuvchi va ulardan jismoniy foydalanish imkoniyatiga ega bo'lgan xodimlar;

4) axborot tizimlari, tarmoqlari va axborotni himoya qilish vositalariga xizmat ko‘rsatuvchi hamda himoya obyektlariga imtiyozli jismoniy va mantiqiy kirish huquqiga ega bo‘lgan administratorlar;

5) Axborot tizimlarini ishlab chiquvchilar (dizaynerlar, dasturlarni ishlab chiquvchilar) bo'lgan bank xodimlari;

6) xonalarga va boshqa himoya vositalariga jismoniy kirish huquqiga ega xavfsizlik xizmati xodimlari (qo'riqlash) va boshqalar.

6.5. Bankning axborot xavfsizligini buzuvchilar tashqi bo'lishi mumkin, ularga quyidagilar kiradi:

1) ishdan bo'shatilgan bank xodimlari;

2) uchinchi tomon tashkilotlarining (sheriklar, nazorat organlari va boshqalar) mijozlari yoki vakillari bo'lgan tashrif buyuruvchilar;

3) shartnoma asosida ishlarni amalga oshiruvchi (pudratchilar, yetkazib beruvchilar, ishlab chiquvchilar va boshqalar), shuningdek autsorsing xizmatlarini ko'rsatadigan uchinchi tomon tashkilotlarining vakillari;

4) tashqi tarmoq yoki aloqa kanallari orqali bank axborot tizimlariga kirish imkoniyatiga ega bo‘lgan tashqi foydalanuvchilar (mijozlar, hamkorlar, muassislar

va boshqalar);

5) tashqi tarmoq orqali tashqaridan harakat qiluvchi buzg'unchilar va boshqalar.

6.6. Potentsial buzg'unchilarni quyidagi mezonlarga ko'ra tasniflash mumkin:

1) tajriba - axborot texnologiyalari sohasidagi malaka darajasi;

2) qobiliyatning mavjudligi - himoya qilish obyektiga nisbatan funksionallik, huquq va vakolatlar darajasi.

6.7. Axborot texnologiyalari sohasidagi tajribaga asoslanib, potentsial qoidabuzarlar quyidagi toifalarga bo'linadi:

1) tajribasiz foydalanuvchi (A toifasi): tashkilotning standart vositalaridan qanday foydalanishni bilmaydi va asosan himoyalangan obyektga ehtiyotsizlik yoki noto'g'ri harakatlar manbai sifatida xavf tug'diradi, ular kamdan-kam uchraydi, lekin noto'g'ri ishlashga yoki noto'g'ri ishlashga olib kelishi mumkin. hatto tizimning ishlamay qolishi, shuningdek, uning beixtiyor harakatlari tashkilotga zarar etkazishi mumkin;

2) ishonchli foydalanuvchi (B toifasi): buzg'unchilarning ushbu toifasi standart vositalardan qanday foydalanishni biladi va himoyalangan ob'ektning ishlashini buzish manbai bo'lishi mumkin, ammo ularning dasturlarini o'rnatishga yoki tashqi resurslardan, shu jumladan Internetdan foydalanishga urinishlar kirishni boshqarish tizimi va axborot xavfsizligi vositalari tomonidan to'xtatilishi;

3) malakali foydalanuvchi (C toifasi): texnik vositalar bilan ishlash va ularga texnik xizmat ko'rsatish bo'yicha yuqori darajadagi bilim va tajribaga ega, axborot tizimlarini dasturlash, loyihalash va ulardan foydalanish sohasida bilimga ega, shuningdek tuzilishi, funksiyalari va mexanizmini bilishi himoya vositalarining ta'siri, ularning kuchli va zaif tomonlari.

6.8. Mumkin bo'lgan harakatlarga asoslanib, potentsial buzg'unchi to'rt darajadan biriga tegishli bo'lishi mumkin:

1) buzg'unchining imkoniyatlarining birinchi (past) darajasi oldindan taqdim etilgan ma'lumotlarni qayta ishlash funksiyalari bilan belgilangan to'plamdan vazifalarni ishga tushirish bilan tavsiflanadi;

2) ikkinchi (o'rta) daraja birinchi darajali foydalanuvchilarning imkoniyatlarini, shuningdek, qo'shimcha ravishda axborotni qayta ishlashning yangi funksiyalari bilan o'z dasturlarini yaratish va ishga tushirish qobiliyatini o'z ichiga oladi;

3) uchinchi (yuqori) daraja, himoyalangan obyektning ishlashini nazorat qilish, ya'ni asosiy dasturiy ta'minot, uning tarkibi, konfiguratsiyasi va ishlashiga ta'sir qilish qobiliyatiga ega;

4) to'rtinchi (juda yuqori) daraja, himoya qilish obyektlarining texnik vositalarini loyihalash, joriy etish va ta'mirlashni amalga oshiruvchi shaxslarning ma'lumotlarni qayta ishlashning yangi funktsiyalariga ega bo'lgan apparat va dasturiy ta'minotni himoya qilish tizimiga kiritishgacha bo'lgan barcha imkoniyatlari bilan tavsiflanadi.

6.9. Bankning har bir potentsial buzilishi uchun Bankning axborot

xavfsizligini buzg'unchi modeli quyidagilarni o'z ichiga oladi:

1) tajriba toifasi;

2) harakatlarni amalga oshirish imkoniyati darajasi;

3) buzg'unchining xususiyatlari - uning imkoniyatlari va taklif qilingan harakatlari;

4) axborot xavfsizligini buzish uchun foydalanishi mumkin bo'lgan ta'sir qilish usullari, usullari va vositalari;

5) buzg'unchilik sabablari (xato, mas'uliyatsizlik, o'zini-o'zi tasdiqlash yoki xudbin manfaat);

6) u ta'sir qilishi mumkin bo'lgan himoya obyektlari;

7) buzg'unchiga nisbatan asosiy cheklovchi choralar (qarshi choralar).

6.10. Buzg'unchi quyidagi usullar va vositalardan foydalanishi mumkin:

1) ma'lumotlar va ma'lumotlarni yig'ish;

2) passiv tutib olish vositalari;

3) axborot tizimiga yoki uni himoya qilish tizimiga kiritilgan standart vositalardan foydalanish va ularning kamchiliklari;

4) faol ta'sir qilish vositalaridan foydalanish (qo'shimcha vositalarni o'zgartirish va ulash, ma'lumotlarni uzatish kanallariga ulanish, dasturiy xatcho'plarni amalga oshirish, maxsus instrumental texnologik dasturlar va yordamchi dasturlardan foydalanish).

Bankning potentsial buzg'unchilar modeli 6-jadvalda keltirilgan.

6-jadval. Bank axborot xavfsizligini potentsial buzug'unchilarning modellari

Model ko'rsatkichlari	Tavsif
Ichki buzg'unchilar	
1. Axborot tizimlari va tarmoqlarining ro'yxatdan o'tgan (vakolatli) foydalanuvchilari (to'g'ridan-to'g'ri foydalanuvchilar) bo'lgan xodimlar	
Tajriba	**B toifasi (ishonchli foydalanuvchi)**
Imkoniyatlar	**birinchi (past) daraja**
Xarakteri	Asosan o'z vakolatlarini kengaytirish va axborot xavfsizligi choralarini engib o'tishga urinishlar bilan bog'liq bo'lgan tahdidlarni amalga oshirish imkoniyati mavjudligi himoya obyektida ehtiyotsizlik yoki noto'g'ri harakatlar manbai bo'lishi mumkin, shuningdek, ular axborotning mavjudligi bilan tavsiflanadi. va himoyalangan ma'lumotlarning sizib chiqishi ehtimoli
Ta'sir qilish usullari, imkoniyat va vositalari	himoya qilinadigan obyektning standart dasturiy va texnik vositalaridan, ular bilan o'zaro ta'sir qilish vositalaridan yoki himoya qilish tizimining vositalaridan, shuningdek ularning kamchiliklaridan foydalanish
Motivlar	xato, mas'uliyatsizlik yoki xudbin qiziqish
Ta'sirga duchor bo'lgan himoya obyektlari	axborot tizimlari, tarmoq, ish stantsiyalari, dasturiy ta'minot va raqamli shakldagi axborot (ma'lumotlar).
Cheklovchi choralar va qarshi choralar	huquqlarni differensiallashtirish va himoya qilinadigan obyektlarga kirishni nazorat qilish; axborot tizimlarida xodimlarning harakatlarini qayd etish; axborotning chiqib ketish kanallarini kamaytirish yoki nazorat qilish; xodimlar tomonidan konfidensial ma'lumotlarni oshkor qilmaslik qoidalariga rioya qilish
2. Axborot tizimlari va tarmoqlaridan foydalanuvchi bo'lmagan ishchilar (bino va xonalarga xizmat ko'rsatuvchi texnik xodimlar va boshqalar).	
Tajriba	**A toifasi (tajribasiz foydalanuvchi)**
Imkoniyatlar	**birinchi (past) daraja**
Xarakteri	ushbu turdagi buzg'unchining tahdidlarini amalga oshirish imkoniyatlari himoya obyektiga ruxsatsiz jismoniy kirishni olish bilan cheklanadi yoki ular asosan himoya obyektiga beparvo yoki noto'g'ri harakatlar manbai bo'lib xizmat qiladi, bu tizimning ishdan chiqishiga yoki hatto ishlamay qolishiga olib kelishi mumkin
Ta'sir qilish usullari, imkoniyat va vositalari	ma'lumot to'plash yoki passiv tutib olish vositalaridan foydalanish
Motivlar	xato yoki mas'uliyatsizlik

Ta'sirga duchor bo'lgan himoya obyektlari	tashkilotning har qanday moddiy aktivlari, shuningdek moddiy yoki nomoddiy (bilim) shakldagi ma'lumotlar
Cheklovchi choralar va qarshi choralar	himoya obyektlarini joylashtirish bo'yicha talablarni bajarish; himoya obyektiga nisbatan ruxsatsiz jismoniy kirish va harakatlarning oldini olish va oldini olishga qaratilgan rejim va tashkiliy-texnik chora-tadbirlardan foydalanish; kadrlarni tanlash va joylashtirish; himoya ob'ektlari joylashgan binolarga kirishni ta'minlash va boshqarish.
3. Tashkilotning texnik vositalariga xizmat ko'rsatadigan xodimlar	
Tajriba	**C toifasi (malakali foydalanuvchi)**
Imkoniyatlar	**ikkinchi (o'rta) daraja yoki uchinchi (yuqori) daraja**
Xarakteri	himoya obyektining texnik va dasturiy vositalariga ruxsatsiz jismoniy kirishning mavjudligi, ammo ularning ro'yxatdan o'tgan foydalanuvchisi emas
Ta'sir qilish usullari, imkoniyat va vositalari	ma'lumotlarni yig'ish, passiv ushlash vositalari, doimiy vositalardan foydalanish yoki faol ta'sir qilish vositalaridan foydalanish
Motivlar	xato yoki o'zini tasdiqlash
Ta'sirga duchor bo'lgan himoya obyektlari	ular xizmat ko'rsatadigan texnik vositalar (axborotni qayta ishlash va saqlash vositalari, tarmoq uskunalari va axborotni himoya qilish vositalari), shu jumladan ularda o'rnatilgan dasturiy ta'minot va ularda saqlanadigan ma'lumotlar
Cheklovchi choralar va qarshi choralar	himoya qilinadigan obyekt joylashgan xonalarga jismoniy shaxslarni kiritish uchun cheklovchi omillardan foydalanish; ish tartibini nazorat qilish, ishlarni nazorat qilish; faqat xizmat ko'rsatilayotgan texnik jihozlarga kirishni ta'minlash; ishni tugatgandan so'ng asbob konfiguratsiyasi va ma'lumotlarining yaxlitligini tekshirish.
4. Tashkilotning tarmoqlari, axborot tizimlari va axborot xavfsizligi vositalariga xizmat ko'rsatuvchi administratorlar	
Tajriba	**C toifasi (malakali foydalanuvchi)**
Imkoniyatlar	**uchinchi (yuqori) yoki to'rtinchi (juda yuqori) daraja**
Xarakteri	himoyalangan obyektga ruxsat berilgan jismoniy va mantiqiy ruxsatga ega bo'lgan va imtiyozli foydalanuvchilar guruhining a'zolari, ya'ni. himoyalangan obyektning ishonchli xodimlari qatoriga kiradi va himoyalangan obyekt tarkibiy qismlarining ichki holatiga ta'sir qilish orqali tahdidni amalga oshirish uchun keng imkoniyatlar beriladi.
Ta'sir qilish usullari, imkoniyat va vositalari	standart vositalardan, ularning kamchiliklaridan yoki faol ta'sir qilish vositalaridan foydalanish
Motivlar	xato, o'z-o'zini tasdiqlash yoki xudbin qiziqish

Ta'sirga duchor bo'lgan himoya obyektlari	tashkilotning axborot tizimlari, ularning texnik vositalari, dasturiy ta'minoti, axborot tizimida saqlanadigan va qayta ishlanadigan ma'lumotlar
Cheklovchi choralar va qarshi choralar	himoya obyektiga kirishda ushbu ishchilarning harakatlarini hisobga olish va nazorat qilish; imtiyozli foydalanuvchi boshqaruv tizimini qo'llash; xavfsizlikni nazorat qilish tizimi tomonidan ushbu toifadagi bosqinchining kirishni nazorat qilish va axborot xavfsizligi choralari bo'yicha belgilangan qoidalarni chetlab o'tishga bo'lgan barcha urinishlarini qayd etish, xavfsizlik tizimi tomonidan ushbu urinishlarni blokirovka qilish; ushbu toifadagi ishchilarga nisbatan javobgarlik choralarini kuchaytirish
5. Axborot tizimlarini ishlab chiquvchi tashkilot xodimlari (dizaynerlar, dasturlarni ishlab chiquvchilar)	
Tajriba	**C toifasi (malakali foydalanuvchi)**
Imkoniyatlar	**uchinchi (yuqori) yoki to'rtinchi (juda yuqori) daraja**
Xarakteri	axborot tizimining amaliy dasturini ishlab chiqishda yoki dastur dasturining normal ishlashini buzish, ruxsatsiz yoki ma'lumotlarning tarqalishi bilan bog'liq noqonuniy xatti-harakatlarni amalga oshirish uchun e'lon qilinmagan funksional imkoniyatlarni (xatcho'plarni) o'rnatishda ishlab chiquvchilarning xatolariga olib keladigan tahdidlarni amalga oshirish imkoniyati mavjudligi
Ta'sir qilish usullari, imkoniyat va vositalari	doimiy yoki faol ta'sir qilish vositalaridan foydalanish
Motivlar	xatolar yoki o'z-o'zini tasdiqlash
Ta'sirga duchor bo'lgan himoya obyektlari	axborot tizimlarining dasturiy ta'minoti va tashkilotning axborot tizimlarining o'zi
Cheklovchi choralar va qarshi choralar	ishlab chiqish jarayonida ushbu xodimlarning harakatlarini hisobga olish va nazorat qilish; dastlabki kod analizatorlari yordamida tashkilotning alohida xodimlari tomonidan ishlab chiqilgan dasturlarni tahlil qilish; ishlab chiqilgan dasturning funksionalligini, kirish va chiqish ma'lumotlarini sinovdan o'tkazish; dasturiy mahsulotlarni axborot xavfsizligi talablariga muvofiq sertifikatlash
6. Xavfsizlik xizmati xodimlari (qoravul)	
Tajriba	**A toifasi (tajribasiz foydalanuvchi)**
Imkoniyatlar	**to'rtinchi (juda yuqori) daraja**
Xarakteri	xonalarga va boshqa muhofaza qilish obyektlariga ruxsat berilgan jismoniy kirishning mavjudligi
Ta'sir qilish usullari, imkoniyat va vositalari	passiv ushlash vositalari yoki standart vositalardan foydalanish.

Motivlar	mas'uliyatsizlik yoki xudbin qiziqish
Ta'sirga duchor bo'lgan himoya obyektlari	xonalar, tashkilotning jismoniy himoyalangan moddiy boyliklari
Cheklovchi choralar va qarshi choralar	xonalarga kirishni hisobga olish (videokuzatuv, jurnalga kirish va chiqish); ushbu toifadagi xodimlarga nisbatan javobgarlik choralarini kuchaytirish; tegishli kadrlarni tanlash
Tashqi buzg'inchilar	
1. Tashkilotning ishdan bo'shatilgan xodimlari	
Tajriba	ilgari egallab turgan lavozimiga qarab toifa
Imkoniyatlar	ilgari egallab turgan lavozimiga qarab daraja
Xarakteri	ushbu turdagi tashqi buzg'inchilarning tahdidlarini amalga oshirish imkoniyatlari tashkilotning himoyalangan ma'lumotlarini, shu jumladan ruxsatsiz kirishga erishish yoki axborot xavfsizligi choralarini chetlab o'tish bilan bog'liq texnologik va texnik ma'lumotlarni shaxsiy manfaat olish yoki zarar etkazish maqsadida oshkor qilish yoki ishlatishgacha qisqartiriladi. sobiq tashkilotga zarar yetkazish yoki noqonuniy harakatlar sodir etish
Ta'sir qilish usullari, imkoniyat va vositalari	axborot va ma'lumotlarni to'plash, faol ta'sirdan foydalanish
Motivlar	xudbin qiziqish
Ta'sirga duchor bo'lgan himoya obyektlari	tashkilotdagi faoliyati davomida olingan bilimlar va konfidensial ma'lumotlar
Cheklovchi choralar va qarshi choralar	xodim ishdan bo'shatilgandan keyin konfidensial ma'lumotlarni oshkor qilmaslik bo'yicha majburiyatlarni bajarish; ishdan bo'shatilgandan keyin ularning kirish ma'lumotlaridan foydalanish imkoniyatini istisno qilish; ishdan bo'shatilganda konfidensial ma'lumotlarni, tafsilotlarni va kirish identifikatorlarini, xavfsizlik choralarini va boshqalarni topshirish
2. Uchinchi shaxslarning mijozlari yoki vakillari bo'lgan tashrif buyuruvchilar	
Tajriba	**A toifasi (tajribasiz foydalanuvchi) yoki B toifasi (ishonchli foydalanuvchi)**
Imkoniyatlar	**birinchi (past) daraja**
Xarakteri	Ushbu turdagi tashqi tajovuzkor tahdidlarini amalga oshirish qobiliyati himoyalangan ob'ektga ruxsatsiz jismoniy kirishni qo'lga kiritish bilan bog'liq.
Ta'sir qilish usullari, imkoniyat va vositalari	passiv ushlash vositalari yoki standart vositalar

Motivlar	xudbin qiziqish
Ta'sirga duchor bo'lgan himoya obyektlari	jismoniy himoyalanmagan moddiy boyliklar va axborotni qayta ishlash vositalari
Cheklovchi choralar va qarshi choralar	himoyalangan obyektlarni joylashtirish talablarini bajarish; binolarni xavfsizlik zonalariga bo'lish; xavfsizlik va tashkiliy-texnik chora-tadbirlar majmuidan foydalangan holda ruxsat etilmagan xonalarga (hududlarga) tashrif buyuruvchilarning kirishini cheklash; tashrif buyuruvchilarni nazorat qilish va ro'yxatga olish; tashrif buyuruvchilarga hamrohlik qilish; past xavfsizlik zonalarida tashrif buyuruvchilarni qabul qilish
3. Shartnoma asosida ishlarni bajaruvchi (pudratchilar, yetkazib beruvchilar, ishlab chiquvchilar va boshqalar), shuningdek autsorsing xizmatlarini ko'rsatadigan uchinchi tomon tashkilotlarining vakillari	
Tajriba	**B toifasi (ishonchli foydalanuvchi) yoki C toifasi (malakali foydalanuvchi)**
Imkoniyatlar	**ikkinchi (o'rta) daraja yoki uchinchi (yuqori) daraja**
Xarakteri	Himoya qilinadigan obyektga mantiqiy va jismoniy kirish huquqiga ega bo'lgan, lekin ularning ro'yxatdan o'tgan foydalanuvchisi - himoyalangan ob'ektning apparat va dasturiy ta'minotini ishlab chiquvchisi bo'lmagan, ularni o'rnatish, ishga tushirish, foydalanish paytida texnik xizmat ko'rsatish va hokazolarni amalga oshiradigan huquqbuzarlarning ushbu turining o'ziga xos xususiyati hisoblanadi. maxsus buzg'unchi vositalarga o'rnatilgan ishlash algoritimiga qarab turli harakatlarni amalga oshirishi mumkinligi. Maxsus buzg'unchi vositalarni ishga tushirish himoyalangan obyektning butun hayoti davomida ishlashining istalgan vaqtida sodir bo'lishi mumkin.
Ta'sir qilish usullari, imkoniyat va vositalari	faol vositadan foydalanish
Motivlar	xudbin qiziqish
Ta'sirga duchor bo'lgan himoya obyektlari	ular tomonidan foydalaniladigan va xizmat ko'rsatadigan apparat va dasturiy ta'minot
Cheklovchi choralar va qarshi choralar	ish tartibini nazorat qilish; ushbu ish davomida tashkilot vakilining mavjudligi; faqat himoyalangan obyektning zarur vositalariga kirishni ta'minlash va ushbu kirishni nazorat qilish; mahsulotni loyihalashda texnik talablarga rioya qilish; "oq xaker" tamoyilidan foydalangan holda zaiflik testi; ishni tugatgandan so'ng asbob konfiguratsiyasi va ma'lumotlarining yaxlitligini tekshirish

4. Tashkilotning axborot tizimlariga tashqi tarmoq orqali kiruvchi tashqi foydalanuvchilar	
Tajriba	**B toifasi (ishonchli foydalanuvchi)**
Imkoniyatlar	**birinchi (past) daraja**
Xarakteri	Tashkilotning axborot tizimlariga mantiqiy ruxsatga ega bo'lish, ularning ro'yxatdan o'tgan foydalanuvchisi bo'lish, ular tomonidan yuzaga kelishi mumkin bo'lgan tahdidlar, asosan, faqat standart dasturiy ta'minot va texnik vositalardan foydalangan holda o'z vakolatlarini kengaytirish va axborot xavfsizligi choralarini yengib o'tishga urinishlar bilan bog'liq. Asosiy motiv hisoblanadi.
Ta'sir qilish usullari, imkoniyat va vositalari	himoya qilinadigan obyektning standart dasturiy ta'minoti va texnik vositalaridan va ular bilan o'zaro ta'sir qilish vositalaridan foydalanish
Motivlar	xudbin qiziqish
Ta'sirga duchor bo'lgan himoya obyektlari	kirish huquqi berilgan axborot tizimlari
Cheklovchi choralar va qarshi choralar	huquqlarni farqlash va himoya obyektlariga kirishni boshqarish; axborot tizimlarida foydalanuvchilarning harakatlarini hisobga olish
5. Himoya obyektiga ruxsatsiz mantiqiy kirish huquqini olgan buzg'unchilar tashqarida tashqi tarmoq orqali, himoya tizimini chetlab o'tish	
Tajriba	**C toifasi (tasniflangan foydalanuvchi)**
Imkoniyatlar	**ikkinchi (o'rta), uchinchi (yuqori) yoki to'rtinchi (juda yuqori) daraja**
Xarakteri	tizimdagi maxsus dasturiy-texnik vositalar yoki zaifliklardan foydalangan holda maqsadli harakatlarni amalga oshirish
Ta'sir qilish usullari, imkoniyat va vositalari	faol vositadan foydalanish
Motivlar	xudbin qiziqish yoki o'zini o'zi tasdiqlash
Ta'sirga duchor bo'lgan himoya obyektlari	tashkilotning lokal va korporativ tarmoqlari va ularga ulangan axborot resurslari va axborot tizimlari, shuningdek axborotni qayta ishlash, saqlash va uzatish vositalari.
Cheklovchi choralar va qarshi choralar	ushbu buzg'unchilarning ruxsat etilmagan harakatlarining oldini olish va bostirishga qaratilgan apparat va dasturiy ta'minotni himoya qilish vositalari majmuasidan foydalanish; tarmoqlar va dasturiy ta'minotdagi zaifliklarni aniqlash va oldini olish.

7. AXBOROT XAVFSIZLIGI CHORALARI

7.1. 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.

7.2 *Huquqiy choralar (hujjatlar bilan ta'minlash choralari)*

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

Bankning axborot xavfsizligi sohasidagi normativ-huquqiy bazasi ushbu siyosatning 1.2-qismida ko'rsatilgan O'zbekiston Respublikasining davlat standartlarini, shuningdek axborot xavfsizligini ta'minlash masalalarini tartibga soluvchi Bankning ichki hujjatlarini o'z ichiga olgan normativ-huquqiy va normativ hujjatlarni o' z ichiga oladi.

Bankning axborot xavfsizligini ta'minlash sohasidagi normativ-huquqiy bazasi Axborot xavfsizligi boshqarmasi tomonidan shakllantiriladi va yuritiladi.

Bankning axborot xavfsizligi sohasidagi idoraviy normativ hujjatlari axborot xavfsizligi boshqarmasi tomonidan bankning boshqa manfaatdor bo'linmalari (umumiy xavfsizlik boshqarmasi, axborot texnologiyalari departamenti va boshqalar) bilan birgalikda ishlab chiqiladi (takomillashtiriladi).

Normativ hujjatlar bankning idoraviy normativ hujjatlarida belgilangan qoidalarga muvofiq kelishiladi va tasdiqlanadi. Axborot xavfsizligi sohasidagi bank hujjatlari quyidagi hujjatlar darajasidan 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).

Axborot xavfsizligi bo'yicha idoraviy hujjatlar va ularda ko'rsatilgan talablar axborot xavfsizligi boshqarmasi tomonidan bankning tegishli xodimlariga etkaziladi va ularga qat'iy rioya qilinishi kerak.

Axborot xavfsizligi bo'yicha idoraviy me'yoriy hujjatlarning alohida turlari ushbu Siyosatning ilovalarida keltirilgan.

7.3 Xulqiy va axloqiy (psixologik) axborot himoyasi choralar

7.3.1. 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 axloqiy xulq-atvor qoidalariga rioya qilish.

Xulqiy va axloqiy himoya choralari profilaktika choralari bo'lib, ularga quyidagilar kiradi:

- bank xodimlari o'rtasida tushuntirish ishlari olib borish;
- huquqbuzarlarga nisbatan intizomiy choralarni majburlash va qo'llash;
- xodimlarni rag'batlantirish va rag'batlantirish.

7.3.2. Tushuntirish ishlari Axborot xavfsizligi boshqarmasi tomonidan maxsus darslar yoki individual suhbatlar shaklida amalga oshiriladi. Ushbu tushuntirish ishlarini amalga oshirish uchun Bankning Umumiy xavfsizlik boshqarmasi va Xodimlarni boshqarish departamenti xodimlari jalb qilinishi mumkin.

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 axborot xavfsizligi 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.

Ushbu tushuntirish ishlari ishga joylashish paytida ham, ish bilan ta'minlash paytida ham xodimlarga nisbatan amalga oshiriladi.

Tushuntirish ishlari Bank xodimlarining quyidagi guruhlari uchun alohida olib boriladi:

- axborot tizimlaridan foydalanuvchi Bank xodimlari;

- bank mijozlariga xizmat ko'rsatuvchi xodimlari;

- axborot tizimlari va resurslari, bank axborot infratuzilmasining texnik va texnologik uskunalariga xizmat ko'rsatishni ta'minlaydigan xodimlari;

- texnik xodimlari.

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

Ko'rilayotgan chora-tadbirlar majmui bank xodimlari AXni ta'minlash bo'yicha qoidalar va talablarga, shu jumladan ular buzilgan taqdirda jazo choralariga rioya qilishlari shart bo'lgan shart-sharoitlarni yaratishga qaratilgan.

Qonunbuzarlarga nisbatan bank rahbariyati va vakolatli qo'mitalar tomonidan mehnat shartnomalari doirasida mehnat qonunchiligiga muvofiq tanbeh yoki jarima shaklida intizomiy jazo choralari qo'llanilishi mumkin.

7.3.4 Rag'batlantirish choralari bank xodimlarini to'g'ri xulq-atvorga undaydigan shart-sharoitlarni yaratishga qaratilgan bo'lishi kerak.

7.3.5 Huquqbuzarliklarning oldini olish, ularni sodir etishiga sabab bo'lgan sabab va shart-sharoitlarni bartaraf etish maqsadida bank xodimlari Vazirlar Mahkamasining 2022-yil 14-oktabrdagi "Qo'shimcha to'g'risida"gi 595-son qarori bilan tasdiqlangan Davlat xizmatchilarining odob-axloq qoidalarining namunaviy qoidalariga rioya etishlari shart. "Davlat xizmatchilari tomonidan odob-axloq qoidalariga rioya etilishini ta'minlash chora-tadbirlari" hamda bank Kuzatuv kengashining 2021-yil 25-fevraldagi 7 son bayonnomasi bilan tasdiqlangan Korporativ odob-axloq kodeksi.

7.4 Tashkiliy choralar

7.4.1 Tashkiliy tadbirlar quyidagilarga qaratilgan:

- axborot aktivlarini boshqarish;

- 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 yuritishi va rivojlanishi;

- axborot xavfsizligi hodisalariga javob berish;

- xavfsizlik holatini nazorat qilish va baholash.

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

7.4.2 Axborot aktivlarini boshqarish bo'yicha tashkiliy chora-tadbirlar quyidagilardan iborat:

a) axborot resurslarini va ular bilan bog'liq axborotni qayta ishlash vositalarini aniqlash uchun axborot aktivlarini muntazam ravishda 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.

7.4.3 Bankda axborot aktivlarini inventarizatsiya qilish, hisobga olish, egalik qilish, tasniflash, yorliqlash, reestrni shakllantirish, shuningdek ularni boshqarishning boshqa tartiblari ushbu Siyosatning 11-ilovasida keltirilgan Axborot aktivlarini boshqarish tartibiga muvofiq amalga oshiriladi.

Xavfsizlik obyektlari va axborot aktivlarini aniqlash uchun inventarizatsiya Axborot xavfsizligi boshqarmasi tomonidan Umumiy xavfsizlik boshqarmasi va Axborot texnologiyalari departamenti bilan birgalikda tashkil etiladi va amalga oshiriladi. Inventarizatsiya natijalariga ko'ra, agar kerak bo'lsa, himoya obyektlari ro'yxatiga, axborot aktivlari (resurslari) reestriga va Bankning konfidensial ma'lumotlari ro'yxatiga o'zgartirish va qo'shimchalar kiritiladi. Bundan tashqari, inventarizatsiya natijalariga ko'ra, xonalarning ro'yxati, ularga kiritilgan texnik va dasturiy vositalar 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 Axborot xavfsizligi boshqarmasi tomonidan amalga oshiriladi.

7.4.4. 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 kompetentsiya darajasining bank tomonidan ishga qabul qilishda belgilangan malaka va qobilyat talablariga muvofiqligini tekshirish;

b) ishga joylashishda:

- mehnat shartnomalarida axborot xavfsizligi sohasida javobgarlikni belgilash;

- ushbu Siyosat bilan tanishish;

- ish tavsiflarida belgilangan axborot xavfsizligi sohasidagi vakolatlar, majburiyatlar va javobgarlik, shuningdek axborot xavfsizligi bo'yicha axborot

xavfsizligi talablarini bajarmaganlik uchun bankda rag'batlantirish va intizomiy jazo choralari bilan xabardor qilish;

v) ish paytida:

- xabardorlikni oshirish, ta'lim va trening;
- axborot xavfsizligini ta'minlash uchun mas'ul bo'lgan xodimlarni qayta tayyorlash va malakasini oshirish (zaruri kompetentsiyalarni 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 Axborot xavfsizligi boshqarmasi tomonidan belgilanadi.

Mehnat shartnomalarida axborot xavfsizligi sohasidagi majburiyatlar va majburiyatlarni aniqlash, shuningdek ular to'g'risida bank xodimlarini xabardor qilish Xodimlarni 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 xavfsizligi boshqarmasi bank xodimlari uchun axborot xavfsizligi sohasida ularning xabardorligini oshirish va ularning majburiyatlari va majburiyatlarini tushunish maqsadida treninglar va seminarlar o'tkazadi.

Xodimlarning xabardorlik darajasini tekshirish yoki baholash axborot xavfsizligi boshqarmasi tomonidan o'tkazilgan treninglar, treninglar va seminarlar natijalari bo'yicha bank xodimlari va uning alohida mutaxassislarini sertifikatlash, sinovdan o'tkazish va so'roq qilish orqali amalga oshiriladi.

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

- bank axborot xavfsizligi siyosati yoki tartib-taomillarini buzganlarga nisbatan intizomiy javobgarlik belgilash;
- bank xodimlarini axborot xavfsizligi qoidalarini buzishdan cheklash;

- ibni qasddan buzganlik uchun aybdorlarni javobgarlikka tortish;

- xodimlarni axborot xavfsizligi masalalariga mas'uliyatli munosabatda bo'lishga undash va rag'batlantirish.

7.4.6. 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 ko'rsatish zonasi) - tashrif buyuruvchilarni qabul qilish joylari va joylari-bosh ofis va savdo ofislarida mijozlarga xizmat ko'rsatish punkti;

2) o'rta xavfsizlik zonalari (2-xizmat ko'rsatish zonasi) - faqat bank xodimlarining mavjudligiga ruxsat berilgan xonalar va joylar: tarkibiy bo'linmalarning xizmat xonalari va ularga tutash bosh ofis, IT-ofis va savdo ofislari koridorlari;

3) yuqori xavfsizlik zonalari (3-himoyalangan zona) – bank xodimlarining ma'lum bir doirasiga kirishga ruxsat berilgan xonalar va joylar: ma'lumotlar markazining server xonasi, bosh ofisdagi kassa ombori.

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

1) binolar va xonalarga nisbatan:

- Bank Bosh ofisi binosining perimetrini va xizmat ko'rsatish tayanch punktlarini himoya qilishni ta'minlash;

- o'tkazish rejimini tashkil etish (xodimlarning kirish/chiqishidagi va Bosh ofisida avtotransport vositalarining kirish/chiqishidagi nazorat punktlari);

- axborotlashtirish obyektlarining muhim aktivlarini Bosh ofis, IT-ofis va savdo ofislarida nazorat qilinadigan hudud chegarasiga nisbatan mumkin bo'lgan maksimal masofada joylashtirish;

- bankning bosh ofisi va savdo ofislari binosida moddiy boyliklar va mol-mulkni olib kirish va olib chiqish uchun moddiy ruxsatnomalar berish;

- bosh ofis va IT-ofis binosida (2-zona) va/yoki ofis xonalarida, savdo ofislarida mehmonlarni kuzatib borish;

-3-zonaning himoyalangan xonalariga qabul qilingan shaxslar ro'yxatini aniqlash.

2) axborotni qayta ishlash, saqlash, uzatish va himoya qilish vositalariga nisbatan:

- vositalarni himoyalangan xonalarda joylashtirish;

- qulflanadigan kommutatsiya shkaflariga vositalarni o'rnatish;

- uskunaning tashqi korpusida qulflar, bir martali ishlatiladigan, muhrlar, himoya yopishqoq lentalar yoki himoya va gologrаfik yorliqlar yoki ruxsatsiz jismoniy kirish faktlarini aniqlashning boshqa vositalaridan foydalanish;

3) qog'oz ko'rinishidagi konfidensial ma'lumotlarga nisbatan:

- seyflar, qulflanadigan temir shkaflar va boshqa himoyalangan omborlardan foydalanish;

- ularni jurnallarda qayd etish.

4) Elektr ta'minoti kabellari va tarmoq kabellari bilan bog'liq holda, ushbu Siyosatning 9-bo'limida ko'rsatilgan ma'lumotlarni ushlab qolish va ularga zarar yetkazilishining oldini olish uchun ularni buzishdan himoya qilish uchun tashkiliy choralar qo'llaniladi.

Bosh ofis binosi va hududiy savdo ofislari qo‘riqlanishi shartnoma asosida Milliy gvardiya tomonidan ta’minlanadi.

Bankga kirish tartibi Bank Boshqaruvining 2020-yil 24-sentabrdagi 7 - son bayonnomasi bilan tasdiqlangan Bankdagi kirish tartibi qoidalariga muvofiq amalga oshiriladi.

7.4.8. Konfidensial ma'lumotlarni himoya qilish bo'yicha tashkiliy chora-tadbirlar quyidagilarni o'z ichiga oladi:

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

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

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

4) Bank kontragentlari bilan tuzilgan shartnomalarda konfidensial ma'lumotlarni oshkor qilish yoki ular bilan oshkor qilmaslik to'g'risida bitimlar tuzish uchun shartlar, talablar, majburiyatlar va javobgarlikni aniqlash (oshkor etmaslik to'g'risidagi bitim, NDA);

5) Konfidensial ma'lumotlar va ularning moddiy tashuvchilari uchun konfidensial griflardan foydalanish;

6) Konfidensial ma'lumotlarga ega tashuvchilarda ma'lumotlarni ro'yxatga olish va hisobga olish;

7) 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;

8) 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;

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

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

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

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

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

Himoya qilinishi lozim bo‘lgan axborot bilan ishlash tartibi Bosh vazir o‘rinbosarining 2006 yil 5 dekabrdagi qarori bilan tasdiqlangan, tarqatilishi cheklangan, konfidensial bo‘lmagan ma’lumotlarni o‘z ichiga olgan hujjatlar, fayllar va nashrlarni hisobga olish, muomala qilish va saqlash tartibi to‘g‘risidagi yo‘riqnomaga muvofiq amalga oshirilishi kerak. O‘zbekiston Respublikasining Davlat sirlarini himoya qilish masalalari bo‘yicha idoralararo komissiyasi raisining, shuningdek, Bank Boshqaruvining 2022-yil 2-dekabrdagi 32-son bayoni tarqatilishi cheklangan ma’lumotlarni (XFU) o‘z ichiga olgan hujjatlar va fayllarni hisobga olish, yuritish va saqlash tartibi to‘g‘risidagi yo‘riqnomasi tasdiqlandi.

Konfidensial ma’lumotlarni qayta ishlashda Bank xodimlari bank Boshqaruvining 2022-yil 2-dekabrdagi 32-son bayonnomasi bilan tasdiqlangan Tijorat siri (konfidensiallik) rejimiga rioya qilish to‘g‘risidagi nizomga amal qilishlari shart. Bank Boshqaruvining 2023-yil 16-maydagi 7-1-son bayonnomasi bilan tasdiqlangan “Anor Bank” AJ xodimlarining shaxsiy ma’lumotlarini qayta ishlash tartibi to‘g‘risidagi nizom.

7.4.9. Axborotni himoya qilish tizimi va vositalarini yaratish, faoliyat yuritishi va rivojlanishi nuqtai nazaridan quyidagi tashkiliy chora-tadbirlar amalga oshiriladi:

a) Bank 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;

v) 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) axborotni himoya qilish vositalarini joriy etishda tajriba-foydalanish va qabul-topshirish sinovlarini o'tkazish;

e) himoya tizimini boshqarish (boshqaruv), shu jumladan konfiguratsiya va sozlamalarni nazorat qilish, ishlash qobiliyatini tiklash, dasturiy ta'minot yangilanishini o'rnatish, operatsion hujjatlarni sozlash, xavfsizlik hodisalarini nazorat qilish, nazorat qilish protseduralari va natijalarini hujjatlashtirish;

s) faoliyatdagi kamchiliklar aniqlangan va xavfsizlikni ta 'minlagan taqdirda axborotni muhofaza qilish tizimini takomillashtirish bo' yicha takliflar tayyorlash va kiritish.

Bankda axborotni himoya qilish tizimi va vositalarini yaratish, ulardan

foydalanish va rivojlantirish bo‘yicha ushbu bandda ko‘rsatilgan tashkiliy chora-tadbirlar Bankning Axborot xavfsizligi boshqarmasi shuningdek, Axborot texnologiyalari departamenti bilan hamkorlikda amalga oshiriladi.

7.4.10. Bank axborot xavfsizligi hodisalariga munosabat bildirish bo‘yicha mazkur Siyosatning 8-bo’limida belgilangan tashkiliy chora-tadbirlarni amalga oshiradi.

Nazorat va xavfsizlikni baholashning tashkiliy chora-tadbirlari quyidagi maqsadlarda qo'llaniladi:

- AXBTning zaif tomonlari va kamchiliklarini aniqlash;
- tahdidlardan himoya qilish obyektlarini muhofaza 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;
- bankning axborot xavfsizligi maqsadlariga erishishini baholash va boshqalar.

Xavfsizlik holatini nazorat qilish va baholash uchun quyidagi tashkiliy chora-tadbirlar ko'rilmoqda:

1) himoya qilish obyektlarini himoya qilish darajasini baholash, shuningdek ushbu Siyosatning yangilanishi va samaradorligini baholash uchun ichki va tashqi auditlarni o'tkazish;

2) ko'rilgan tashkiliy, texnik va boshqa himoya choralari samaradorligini baholash shuningdek, audit natijalari bo'yicha aniqlangan kamchiliklarni bartaraf etish.

Ichki auditning davomiyligini yiliga kamida 1 marta, tashqi audit esa - uch yilda kamida 1 marta.

Ichki audit Axborot xavfsizligi boshqarmasi tomonidan, agar kerak bo'lsa, Umumiy xavfsizlik boshqarmasi va Axborot texnologiyalari departamenti mutaxassislarini jalb qilgan holda amalga oshiriladi. Axborot xavfsizligining tashqi auditini o'tkazish uchun bunday auditni o'tkazishga vakolatli uchinchi tomon tashkilotlari jalb qilinadi.

Tekshiruv natijalari hujjatlashtirilishi kerak, unda quyidagilar 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.

Axborot xavfsizligi boshqarmasi audit va boshqa tekshirishlar natijalariga ko‘ra aniqlangan zaifliklar, kamchiliklar va nomuvofiqliklarni bartaraf etish hamda himoya samaradorligini oshirish bo‘yicha chora-tadbirlar yoki choralar ko‘rishi kerak.

7.5 Texnologik (texnik) tadbirlar

7.5.1. Bank axborot xavfsizligini ta'minlash bo'yicha texnologik (texnik) chora-tadbirlar quyidagilarga qaratilgan:

- ma'lumotlarni saqlash xavfsizligini ta'minlash, uni sizib chiqishi va yo'qolishi, axborot tashuvchi vositalari va saqlash qurilmalarining o'g'irlanishi yoki yo'qolishi, ma'lumotlarning buzilishidan himoya qilish;

- 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;

7.5.2. Bank DSt ISO/IEC 27040:2018 "Axborot texnologiyalari" Xavfsizlik usullari. Ma'lumotlarni saqlash xavfsizligi"ga muvofiq ma'lumotlarni xavfsiz saqlash, ularni chiqib ketishi va yo'qotishdan himoya qilish, saqlash vositalari va qurilmalarining o'g'irlanishi yoki yo'qolishi, ma'lumotlarning buzilishi bo'yicha choralar ko'rishi kerak.

Axborot xavfsizligi choralariga quyidagilar kiradi:

- saqlash himoya obyektlari va ma'lumotlarni tashuvchi vositalarini ruxsatsiz kirishdan himoya qilish;

- axborot tashuvchi vositalari va axborotni saqlash qurilmalarini to'g'ri va nazorat ostida yo'q qilish;

- saqlash qurilmalarini jismoniy himoya qilish;

-ma'lumotlarni saqlash qurilmalariga kirishda autentifikatsiya va monitoring vositalaridan foydalanish;

- qurilmalardagi ma'lumotlarni muntazam ravishda zaxiralash.

Ma'lumotlarning ishonchli himoyasini ta'minlash uchun bank quyidagi texnik (texnologik) choralarni ko'rishi shart:

- muhim saqlash resurslarini almashish;

- ma'lumotlarni zaxiralash;

- muhim axborot tizimlari ma'lumotlarini masofaviy, favqulodda vaziyatlarga chidamli onlayn aks ettirish;

- ma'lumotlarning yagona nusxasi atrofida xatoga chidamli ilovalar va tegishli tizimlarni klasterlash (klasterlash);

- korporativ konfidensial ma'lumotlarni uzoq muddatli saqlash;

- ma'lumotlar bazasi va fayl tizimlarini taqsimlash;

- tezkor tiklash (zaxiralash) va arxivlash uchun ma'lumotlarni saqlashni ta'minlash.

Ma'lumotlarga chidamlilik strategiyasining bir qismi sifatida siz:

-falokat oqibatlarini bartaraf etish rejalarida ma'lumotlarni tiklash choralarini ko'rish;

- zaxira ma'lumotlar asosiy ma'lumotlar saqlanadigan joydan geografik jihatdan uzoqda joylashgan ma'lumotlar omborlarida saqlanadi.

Foydalanish, boshqarish, texnik xizmat ko'rsatish, sozlash va yo'q qilish bilan bog'liq texnologik (texnik) ma'lumotlarni himoya qilish choralari:

- saqlash obyektining uzluksiz ishlashiga qaratilgan operatsiyalar;
- saqlash infratuzilmasidagi resurslarni kuzatish va ularni taqsimlashga qaratilgan administrator faoliyati, shuningdek saqlashni boshqarish uchun zarur bo'lgan barcha tadbirlar;
- ta'mirlash va modernizatsiya ishlari bilan bog'liq texnik xizmat ko'rsatish;
- muayyan dasturiy ta'minot profillarini o'rnatish va tizimlarni ishlashga tayyorlash;
- axborot tashuvchisi saqlashdan uzilganda yoki tashuvchidagi ma'lumotlarga kirish imkoni bo'lmaydigan tarzda o'zgartirilganda ma'lumotlarning konfidensialligini saqlashga qaratilgan yo'q qilish choralari.

7.5.3 Quyidagi ma'lumotlar himoyalangan bo'lishi kerak:

- ABT ma'lumotlar bazasi;
- RBS BSS, ELMA, Wings, BillMaste, AGC (ADPMS), Anorhub, Qlik Sense, Confluence, Gitlab, Jira, Keycloak, MerchantCabinet, ServiceDesk, Verifix, WEBIM, Superset, 1C va boshqa axborot tizimlarining ma'lumotlar bazasi;
- axborot almashish tizimlarining ma'lumotlar bazasi: korporativ elektron pochta, korporativ messenjer, elektron hujjat aylanish tizimi;
- rasmiy veb-sayt ma'lumotlar bazasi;
- domen boshqaruvchisi server sozlamalari va ma'lumotlar bazasi;
- axborot xavfsizligi vositalarining sozlamalari va ma'lumotlar bazalari – tarmoqlararo ekran va IDPS vositasi, DLP tizimlari, operativ xotira, antivirus va boshqalar;
- tarmoq uskunalarini sozlash.

Belgilangan ma'lumotlar server xotirasida saqlanadi va uning zaxira nusxalari ma'lumotlarni saqlash tizimida, zaxira serverlar ma'lumotlar bazasida va lenta disklarida (elektron arxivda) saqlanadi.

7.5.4 7.5.3-bandda ko'rsatilgan axborot tizimlari ma'lumotlari va vositalarining zaxira nusxalarini saqlash uchun SAN saqlash tarmog'iga ulangan ma'lumotlarni saqlash tizimi qo'llaniladi.

Server ma'lumotlar bazasini saqlashda, shuningdek ma'lumotlarni saqlash tizimida axborot tizimi ma'lumotlarining ishonchliligini (xavfsizligini) ta'minlash uchun RAID qo'llaniladi.

7.5.5 Jismoniy ma'lumotlarni himoya qilishni ta'minlash uchun barcha serverlar va ma'lumotlarni saqlash tizimlari, shuningdek, lenta drayvlari bankning asosiy va zaxira ma'lumotlar markazlarining jismoniy himoyalangan server xonasida joylashgan bo'lib, ularga kirish ruxsatsiz shaxslar tomonidan cheklangan.

ABT dastur serverlari va ma'lumotlar bazalarini masofaviy, favqulodda vaziyatlarga chidamli onlayn aks ettirishni ta'minlaydi. Asosiy ABT serverlari asosiy ma'lumotlar markazida (Bank bosh ofisi), zaxira ABT serverlari esa geografik masofaviy zahiraviy ma'lumotlar markazida ("O'zbektelekom" AK Toshkent shahridagi ATS-233 ma'lumotlar markazi) joylashgan. Asosiy ABT serverining ma'lumotlar bazasi doimiy ravishda zaxira ma'lumotlar markazidagi

zaxira ABT ma'lumotlar bazasi serveriga takrorlanadi. Asosiy va zaxira ma'lumotlar markazlarining ABT ma'lumotlar bazalari to'g'ridan-to'g'ri ma'lumotlar markazlari o'rtasida tashkil etilgan optik tolali aloqa liniyasi (OTAL) orqali ulanadi.

7.5.6 SAN saqlash tarmog'i Fiber Channel (FC) texnologiyasi asosida qurilgan bo'lib, unga barcha asosiy ma'lumotlar bazasi serverlari va boshqa axborot tizimlari, ma'lumotlarni saqlash tizimlari, lenta drayvlari va ma'lumotlarni zaxiralash va tiklash tizimlari ulanishi mumkin. SAN tarmog'i asosiy ma'lumotlar markazining server xonasida ikkita SAN kommutatori asosida tashkil etilgan.

Bundan tashqari, asosiy ma'lumotlar markazida DMZ demilitarizatsiya zonasi alohida VLAN shaklida tashkil etilgan bo'lib, unda axborot tizimlari va resurslari serverlari shuningdek, tashqi Internetga ulangan ma'lumotlar almashinuvi tizimlari serverlari, xususan, korporativ elektron pochta, bankning rasmiy veb-sayti, Internet-banking resurslari, mobil banking kiradi.

7.5.7 Muhim axborot tizimlarining zahira nusxalarini uzoq muddatli saqlash uchun bank lenta ma'lumotlar diskidan (lenta kutubxonasi) foydalanadi. Lenta tashuvchidan foydalangan holda muhim axborot tizimlari serverlari va ma'lumotlar bazalarining elektron arxivi elektron arxivni saqlash muddati kamida 1 yil bo'lgan holda shakllantiriladi.

7.5.8 Bank xodimlari Bosh ofisning lokal simli tarmog'i orqali axborot tizimlariga ulangan. Bankning masofaviy IT-ofisi va savdo ofislari xodimlari IT-ofis va savdo ofislarini Bosh ofisga ulash uchun tashkil etilgan xavfsiz VPN IPSec kanallaridan foydalangan holda korporativ tarmoq orqali bank axborot tizimlariga ulanadi.

Axborot tizimlariga kirishda foydalanuvchilar domen kontrolleri serverida, shuningdek, login va paroldan foydalangan holda axborot tizimlarida avtorizatsiya qilinadi.

Foydalanuvchilar xavfsiz https ulanishlari orqali bankning axborot tizimlariga ulanadi.

7.5.9 Axborot tizimlari administratorlari shuningdek, Axborot texnologiyalari departamenti xodimlari bo'lgan ma'lumotlar bazasi administratori bankning aniq axborot tizimlariga biriktirilgan. Belgilangan administratorlar quyidagilarni ta'minlaydi:

- axborot tizimining serverlarini sozlash va jihozlash, server saqlash tizimi va ma'lumotlarni saqlash tizimining barcha xususiyatlarini ko'rish va o'zgartirish;
- hisoblarni yaratish va boshqarish qoidalarini o'zgartirish, axborot tizimi foydalanuvchilari uchun rollar/vakolatlarni yaratish va belgilash;
- serverni saqlash va ma'lumotlarni saqlash tizimlarining parametrlari va konfiguratsiyasini, shuningdek ularning ishlashi va nosozliklari jurnallarini tekshirish;
- axborot tizimining serverlaridan ma'lumotlarni zaxiralash va tiklash;
- ma'lumotlar bazasida yaxlitlikni tekshirish vositalaridan foydalangan holda saqlashdagi ma'lumotlarning yaxlitligini tekshirish.

Axborot xavfsizligi boshqarmasi axborot tizimining ma'lumotlar ombori xavfsizligi bo'yicha auditorning majburiyatlarini bajarishi kerak, ya'ni huquqlar va

vakolatlarni o'rganish, xavfsizlik parametrlari va konfiguratsiyasini tekshirish, shuningdek, audit jurnalini tekshirish imkonini beruvchi xavfsizlik tahlilini o'tkazish.

7.5.10 7.5.8-bandda ko‘rsatilgan administratorlar axborot tizimlariga lokal tarmoq yoki korporativ tarmoq orqali masofaviy kirish uchun VPN shlyuzi tomonidan tashkil etilgan xavfsiz VPN SSL ulanishlaridan foydalangan holda ulanadi. Administratorlar SSH protokoli yordamida tashkil etilgan xavfsiz ulanishlar orqali ulanadilar.

Axborot tizimlariga kirishda administratorlar SSH protokoli yordamida, shuningdek, axborot tizimining o'zida yoki serverlarning operatsion tizimida yoki ma'lumotlar bazasi ma'lumotlar bazasida login va parol yordamida autentifikatsiya qilinadi.

Bundan tashqari, axborot tizimlariga kirishda administratorlar boshqaruv tizimida imtiyozli RAM foydalanuvchilari tomonidan autentifikatsiya qilinadi. Operativ xotira tizimi orqali axborot tizimlarining serverlari va ma'lumotlar bazalariga kirishda administratorlarning kirishi va harakatlari boshqariladi.

7.5.11 Axborot tizimlari ma'lumotlar ombori bilan bog'liq holda audit, buxgalteriya hisobi va xavfsizlik monitoringi amalga oshirilishi kerak:

- saqlash boshqaruvidagi barcha muhim hodisalarni qayd etish;
- hodisalarni ro'yxatga olish ma'lumotlarini saqlash;
- hodisalarni ro'yxatga olish ma'lumotlarini ma'lumotlarni saqlash siyosatiga muvofiq arxivlash va saqlash;
- qurilma vaqtini ishonchli tashqi manba bilan sinxronlash.

Ma'lumotlar omborlaridagi hodisalarni qayd etish va qayd etish uchun standart syslog protokoli qo'llaniladi (tizim jurnali tizimda sodir bo'layotgan hodisalar haqida xabarlarni yuborish va yozish uchun standartdir).

Ma'lumotlar ombori xavfsizligini tekshirish, hisobga olish va monitoring qilish Axborot xavfsizligi boshqarmasi tomonidan, shu jumladan server ishini monitoring qilish tizimi va SIEM hodisalarini monitoring qilish tizimi orqali amalga oshiriladi.

Xavfsiz ma'lumotlarni saqlash siyosatining aniqlangan buzilishlari axborot xavfsizligi hodisalari jurnalida qayd etilishi kerak.

7.5.12 Axborot tashuvchisi va ma'lumotlarni saqlash vositalaridagi ma'lumotlarni o'z-o'zidan yo'q qilish ushbu Siyosatning 7-ilovasida keltirilgan tashuvchi saqlash vositalari, mobil qurilmalar, ma'lumotlarni saqlash qurilmalari bilan ishlashda xavfsizlik qoidalariga muvofiq amalga oshiriladi.

7.5.13 Serverlar va ma'lumotlarni saqlash tizimlarida axborot tizimlari ma'lumotlarini himoya qilishni kuchaytirish uchun axborot tizimlari administratori qo'shimcha ravishda quyidagi choralarni ko'rishi kerak:

- keraksiz va foydalanilmagan dasturiy ta'minotni olib tashlash;
- keraksiz hisoblarni o'chirish;
- o'rnatilgan yoki standart hisoblardagi parollarni qayta nomlash, o'chirish, o'zgartirish;
- foydalanish uchun faqat kerakli tarmoq portlarini ochish;

- ishonchli manbadan eng so'nggi yamoqlarni o'rnatish;
- ishonchli manbadan proshivka yangilanishi;
- zararli dasturlardan himoyani o'rnatish va qo'llab-quvvatlash.

7.5.14 Himoya obyektlarining barqaror va uzluksiz ishlashi uchun quyidagi chora-tadbirlar amalga oshiriladi:

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

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

3) uskunalar va tizimlarning tizim jurnallarini boshqarish va tekshirish;

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

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

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

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

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

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

10) axborotni qayta ishlash obyektlari yaqinida ovqatlanish, ichish va chekish qoidalarini belgilash;

7.5.15. Quyidagi texnik vositalari zahira qilinadi:

- ABT va boshqa axborot tizimlarining serverlari (ma'lumotlar bazalari va ilovalari).
- Korporativ tarmog'ini tashkil qilish uchun foydalaniladigan asosiy kammutatorlar yadrosi;
- asosiy va zaxira ma'lumotlarni qayta ishlash markazlarini korporativ tarmoqqa, tashqi Internet tarmog'iga va Markaziy bankning BTTga ulash chegarasida foydalaniladigan tarmoqlararo ekran va xavfsizlik shlyuzlari.

Axborotni qayta ishlash, saqlash, uzatish va himoya qilish vositalarini, shuningdek aloqa kanallarini zaxiralashga qo'yiladigan talablar ushbu siyosatning 14-ilovasida keltirilgan favqulodda va avariya vaziyatlarda doimiy ishlashni ta'minlash va ishlashni tiklash tartibida belgilanadi.

Ma'lumotlar bazalari va jurnallar (log-fayllar), Bank axborot tizimlarining dasturiy ta'minoti, shuningdek tarmoq uskunalari va axborotni himoya qilish vositalarining sozlanadigan parametrlari (sozlamalari) zaxiralanishi kerak. Bankda ma'lumotlarni zaxiralash va tiklash tizim va amaliy dasturlarni yangilash, shuningdek ushbu siyosatning 4-ilovasida keltirilgan ma'lumotlarni zaxiralash va

tiklash to'g'risidagi Nizomga muvofiq amalga oshiriladi.

Ma'lumotlarning zahiraviy nusxasini ta'minlash uchun ushbu Siyosatning 18-ilovasida ko'rsatilgan ma'lumotlarni zaxiralash va tiklash tizimlari qo'llaniladi.

7.5.16. Uzluksiz elektr ta'minotini ta'minlash uchun quyidagi choralarni ko'rish kerak:

1) Bosh ofisi (asosiy MQIM) binosida, shuningdek xizmat ko'rsatish punktlarida dizel generatori va uzluksiz quvvat manbalaridan foydalaniladi;

2) Asosiy axborot tizimlari, axborot almashish tizimlari, tarmoq uskunalari va axborotni himoya qilish vositalaridan zaxira ma'lumotlar markazida ("O'zbektelekom" AK ATS-233 data markazi) foydalanish, ularda dizel generatori va uzluksiz quvvat manbalaridan foydalangan holda uzluksiz ishlash choralari ko'zda tutilgan.

Bank korporativ tarmog'ini tashqi Internet tarmog'iga va Markaziy bankning BTTga ulash uchun foydalaniladigan aloqa kanallari ortiqcha bo'lishi kerak.

Asosiy telekommunikatsiya uskunalari, ma'lumotlar bazalari, axborot tizimlari serverlari va axborot xavfsizligini ta'minlash vositalari asosiy va zaxira ma'lumotlarni qayta ishlash markazlarida joylashgan bo'lishi kerak.

Bosh ofisi binosidagi zaxira markaz va asosiy markazning server xonasini tashkil etish uchun foydalaniladigan "O'zbektelekom" 233-ATS ma'lumotlar markazi O'zDSt 2875:2014 "ma'lumotlar markazlariga qo'yiladigan talablar" talablariga javob beradi.

- uzluksiz elektr ta'minotini ta'minlash;
- talab qilinadigan iqlim sharoitlarini saqlash (konditsioner tizim);
- yong'in xavfsizligini ta'minlash.

7.5.17. Qayta tiklash choralariga quyidagilar kiradi:

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

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

3) dasturiy ta'minot va ma'lumotlarni zahiradan tiklash;

4) uskunani ta'mirlash yoki almashtirish;

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

Qayta tiklash tadbirlarini amalga oshirish ushbu Siyosatning 14-ilovasida keltirilgan Favqulodda va avariya vaziyatlarda ishlash va tiklashning uzluksizligini ta'minlash rejasi bilan tartibga solinadi.

7.6 Muhandis-texnik choralar

7.6.1. 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) Bosh ofisning zonalari va xizmat ko'rsatish xonalariga eshiklar va boshqa muhandislik vositalari bilan kirish chegaralarini belgilash;

2) xodimlarning identifikatsiya plastik kartochkalaridan foydalanish yoki shaxslarni identifikatsiyalash (face-ID), ko'dli qulflari bilan Bosh ofis SKUD binosi va hududlariga (alohida xizmat ko'rsatish xonalari va xizmat ko'rsatish xonalari bo'lgan yo'laklarga) kirishda foydalanish;

3) 3-zonali xonalarning kirish qismida temir eshiklardan foydalanish;

4) 2-zonaning xizmat ko'rsatish xonalariga kirishda elektron qulflardan foydalanish;

5) bosh ofisda eshik va derazalarni ochish uchun SMT sensorlaridan foydalanish;

6) bosh ofis, IT-ofis va xizmat ko'rsatish punktlarining derazalarini vizual kuzatuvdan himoya qilish vositalari bilan jihozlash (pardalar, jalyuzlilar);

7) Bosh ofis binosi, IT-ofis va xizmat ko'rsatish punktlari koridorlari orqasida video nazorat qilish uchun videokuzatuv tizimidan foydalanish;

8) ruxsatsiz jismoniy kirish faktlarini qayd etish uchun himoyalangan xonalarda xavfsizlik signalizatsiyasi va sensorlarni o'rnatish;

9) hujjatlashtirilgan konfidensial ma'lumotlarni saqlash uchun qulflanadigan temir yonmaydigan shkaflardan foydalanish.

7.7 Dasturiy-apparat choralari

7.7.1. Axborot xavfsizligini ta'minlash bo'yicha apparat-dasturiy choralar quyidagilarga qaratilgan:

- axborotni texnik muhofaza qilishni tashkil etish;
- axborotning kriptografik himoyasini tashkil etish.

7.7.2 Dasturiy ta'minot va apparat ta'minoti choralari quyidagilarni ta'minlash uchun foydalaniladigan apparat, dasturiy ta'minot va texnik ma'lumotlarni himoya qilish vositalaridan foydalanishga asoslanadi:

- tarmoq infratuzilmasi darajasida axborot xavfsizligi (tarmoq xavfsizligi);
- himoyalangan obyektlarga mantiqiy kirishni chegaralash va boshqarish;
- antivirus himoyasi;
- konfidensial ma'lumotlarning chiqib ketishidan himoya qilish;
- xavfsizlikni nazorat qilish va tahlil qilish;
- axborot xavfsizligi hodisalarini kuzatish, boshqarish va boshqalar.

7.7.3. Tarmoq xavfsizligi choralariga quyidagilar kiradi:

1) Bank tarmoq infratuzilmasining xavfsiz arxitekturasini aniqlash;

2) Bank tarmog'ini jismoniy va virtual ravishda ajratish;

3) tarmoq xavfsizligi vositalaridan foydalanish (tarmoqlararo ekran, IDS / IPS hujumlarini aniqlash va oldini olish tizimlari, VPN vositalari, WAF veb-ilovalari uchun tarmoqlararo ekran);

4) xavfsiz kanallar va tarmoq ulanishlarini tashkil etish.

7.7.4 Korporativ tarmog'ining xavfsiz arxitekturasi, uni qurish tamoyillari, shuningdek, xavfsiz kanallar va tarmoq ulanishlarini tashkil etish Ushbu Siyosatning 1- ilovada keltirilgan Korporativ tarmoq va xavfsiz tarmoq ulanishlarini tashkil etish to'g'risidagi nizomda belgilangan.

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

7.7.6 Tarmoq hujumlari va risklar bilan bog'liq axborot xavfsizligi xavflaridan kelib chiqib, bank quyidagi talab va funksiyalarga ega bo'lgan IDPS

apparat va dasturiy tarmoq vositalaridan foydalanishi kerak:

- taqsimlangan tarmoqlar va masofaviy ishchilar uchun SD-WAN va VPN texnologiyalarini qo'llab-quvvatlash;
- barcha protokollar, shu jumladan dastur darajasi bo'yicha tarmoq trafik paketlarini chuqur tahlil qilish;
- barcha tashqi tarmoq trafigini qayta ishlash (paketlarni chuqur tahlil qilish) va uzatishni ta'minlovchi ko'rsatkichlarga ega bo'lish;
- tarmoq trafigida tarmoq tajovuzlarini aniqlash uchun imzoga asoslangan usulni qo'llab-quvvatlash;
- ishlab chiqaruvchidan imzolar bazasini yangilay olish;
- trafikdagi anomaliyalar va tarmoq protokollaridagi anomaliyalar asosida tarmoq trafigiga tarmoq tajovuzlarini aniqlashning xatti-harakatlar usulini qo'llab-quvvatlash;
- shubhali trafikni bloklash va filtrlash;
- veb-tahdidlardan, shu jumladan DNSga asoslangan tahdidlardan, zararli URL-manzillardan himoya qilishni ta'minlash;
- ilovalarni nazorat qilish;
- DoS va DDoS hujumlarini aniqlash va bartaraf etish;
- zararli koddan tarmoq trafigini aniqlash va filtrlash funksiyasiga ega;
- IDPS tarmog'i obyektining yaxlitligini nazorat qilish uchun boshqaruv funksiyasiga ega;
- oddiy tarmoq boshqaruvi (ma'muriyati) protokoliga ega bo'lish;
- aniqlangan va oldini olingan hujumlar haqida xabar berish.

IDPS tarmoq vositasi lokal tarmoqlarni tashqi va korporativ tarmoqlardan himoya qilishi kerak.

Bank tarmoqlararo ekranga o'rnatilgan IDPS tarmoq vositalaridan foydalanadi - IDPS funksiyalariga ega apparat-dasturiy tarmoqlararo ekran.

IDPS funksiyalariga ega tarmoqlararo ekranga ulangan:

- tashqi tarmoqqa ulanganda Bosh ofisning lokal tarmog‘ini tashqi tomondan himoya qilish shuningdek, tashqi tarmoqqa ulanganda zahiraviy ma’lumotlar markazi va IT-ofisning lokal tarmoqlarini himoya qilish;
- korporativ tarmoqqa ulanganda Bosh ofisning lokal tarmog‘ini tashqi tomondan himoya qilish, shuningdek korporativ tarmoqqa ulanganda zahiraviy ma’lumotlar markazi va IT-ofisning lokal tarmoqlarini himoya qilish;
- asosiy ma'lumotlar markazidagi DMZ zonasini shuningdek, asosiy va zaxira ma'lumotlar markazining server segmentini, shuningdek ularni lokal tarmoqlarga ulashda asosiy ma'lumotlar markazidagi protsessor markazini ichkaridan himoya qilish uchun foydaliniladi.

7.7.7 Bank ish stantsiyalari va muhim serverlarda quyidagi funksiyalarga ega HDPSni o'rnatishi kerak:

- jarayonlarni, dasturlarni, fayllarni va operatsion tizimda ishlaydigan registrni kuzatishda kiruvchi faoliyatni aniqlash;
- kiruvchi va chiquvchi trafikni nazorat qilish;
- alohida portlar, dasturlar va IP manzillar uchun parametrlarni o'rnatish;

- tarmoq hujumlaridan himoya qilish shubhali tarmoq faoliyatini tekshirish uchun mo'ljallangan

- ko'p platformali muhitlarni qo'llab-quvvatlash va Linux, Windows, shu jumladan klaster serverlarida ishlaydigan fayl serverlarini himoya qilishni ta'minlash;

- zararli kodli hujumlardan o'zini himoya qilish;

- zaifliklarni qidirish.

HDPS sifatida bank qo'shimcha HDPS funksiyasiga ega bo'lgan virusga qarshi himoya tizimidan foydalanadi.

HDPS ishlashi uchun antivirus ish stantsiyalari va serverlarda mos ravishda sozlangan.

7.7.8. Bank axborot resurslari va tizimlaridan foydalanishni farqlash uchun ushbu Siyosatning 8-ilovasida keltirilgan Axborot resurslariga kirish matritsasini ishlab chiqish qoidalariga muvofiq foydalanish matritsasi ishlab chiqilgan.

7.7.9. Bankda himoyalangan obyektlarga kirishda foydalanuvchilarning autentifikatsiyasi parollar va boshqa identifikatorlar, axborot xavfsiziligi siyosatining 5-ilovasida keltirilgan Parol bilan himoya qilish va foydalanuvchilarni axborot tizimiga autentifikatsiyasi bo‘yicha yo‘riqnoma muvofiq ishlab chiqariladi va foydalaniladi.

7.7.10. Bankda antivirus himoya qilish uchun quyidagi antivirus himoya choralari va vositalari qo‘llaniladi:

1) 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;

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

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

4) axborotni qayta ishlash vositalarida USB portlaridan foydalanishni bloklash.

7.7.11. Jarayonlar, shu jumladan antivirus himoyani tashkil etish va ta'minlash, xodimlar tomonidan zararli dasturlardan himoya qilish talablarini belgilash va bajarish tartibi ushbu siyosatga 6-ilovaga muvofiq antivirus himoya qilish bo'yicha yo'riqnomada belgilangan.

7.7.12 Bank quyidagi texnik himoya vositalaridan foydalanadi:

- Bank xavfsizlik nazorati va tahlili sifatida bankning korporativ tizimidagi zaifliklarni boshqarish tizimi va xavfsizlik skanerlaridan foydalanadi.

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

- Axborot xavfsizligi hodisalarini kuzatish va boshqarish uchun SIEM tizimidan foydalanish ta'minlanadi.

- Imtiyozli foydalanuvchilarning (administratorlarning) harakatlarini nazorat qilish uchun Bank PAM tizimidan foydalanadi.

- Axborotni kriptografik himoya qilish axborotni kriptografik himoya qilish vositalaridan foydalangan holda tashkil etiladi (bundan buyon matnda AKHV deb yuritiladi).

Axborotni texnik himoya qilishning amaldagi usullari va vositalari ushbu siyosatning 23-ilovasiga muvofiq axborotni texnik himoya qilishni tashkil etish qoidalarida keltirilgan.

7.7.13. Bankda yuridik shaxslar bo'lgan bank mijozlari tomonidan BSS DBO tizimining Internet-bankingi orqali raqamli bank xizmatlaridan foydalanishda AKHT elektron raqamli imzoni shakllantirish va tekshirish uchun, shuningdek bank xodimlari tomonidan EHAT foydalaniladi Myanor.uz.

BSS DBO tizimida eri qo'llash uchun bankning raqamli xizmatlarining korporativ mijozlari tomonidan O'zbekiston Respublikasi davlat Soliq qo'mitasining ERI kalitlarini ro'yxatdan o'tkazish markazi tomonidan ishlab chiqarilgan shaxsiy ERI kalitlari va ERI ochiq kalitlari sertifikatlari qo'llaniladi. EHATda Manor.uz shuningdek, bank xodimlari davlat soliq qo'mitasining eri kalitlarini ro'yxatdan o'tkazish markazining yopiq ERI kalitlari va ERI ochiq kalitlari sertifikatlaridan foydalanadilar.

AKHT Bank kotibiyati boshqarmasi xodimlari ulangan elektron pochta bilan himoyalangan elektron pochta tizimida qo'llaniladi.

AKHT qo'shimcha ravishda korporativ tarmoqda va uchinchi tomon axborot tizimlari bilan o'zaro aloqada xavfsiz tarmoq ulanishlarini tashkil qilish uchun ishlatiladi.

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.

Bankda axborotni kriptografik himoyalash usullari va vositalari, axborot xavfsiziligi siyosatining 13-ilovasida keltirilgan Axborotni kriptografik himoya qilishni tashkil etish bo'yicha yo'riqnomaga muvofiq amalga oshiriladi.

7.7.14 Bankda qo'llaniladigan apparat, dasturiy va axborot xavfsizligi vositalari, shuningdek, tarmoq, server uskunalari va dasturiy ta'minotlari ushbu Siyosatning 18-ilovasida keltirilgan.

7.8 Tashqi foydalanuvchilar bilan ishlashda xavfsizlik choralari

7.8.1 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 ham jismoniy, ham mantiqiy, bank mijozlari esa Bank axborot aktivlaridan faqat mantiqiy foydalanishlari mumkin.

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

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

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

2) axborot tizimining uchinchi tomon tashkilotining axborot tizimi bilan o‘zaro hamkorligi;

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

7.8.3 Axborot xavfsizligi choralari raqamli bank xizmatlaridan foydalanuvchi mijozlar bilan ishlashda aniqlanadi (onlayn xizmat).

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

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

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

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

4) 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;

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

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

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

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

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

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

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

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

13) 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.

Uchinchi tomon tashkiloti bilan tuzilgan konfidensial ma'lumotlarni oshkor qilmaslik to'g'risidagi NDA 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 belgilaydi. Shu jumladan, ushbu ma'lumotlarning oshkor etilishi natijasida Bankga yetkazilgan zararning o'rnini qoplash.

NDA shartlari shartnoma muddati davomida va uni bekor qilgandan keyin kamida 5 yil davomida bajarilishi kerak.

7.8.5 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:

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

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

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

Yuqoridagi choralar ikki tomonlama shartnomalarda belgilangan.

Xavfsiz ulanishlarni tashkil etish ushbu 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 ushbu Siyosatga 2-ilovaga muvofiq tarmoq infratuzilmasi va tarmoqlararo ekran darajasida axborot xavfsizligini ta'minlash to'g'risidagi nizomga muvofiq tarmoqlararo ekran choralari qo'llanilishi kerak.

7.8.6. ABT uchinchi tomon axborot tizimlari bilan o'zaro aloqada bo'lganda, quyidagi choralar ko'riladi:

a) ABT ni uchinchi tomon tashkilotlarining axborot tizimlariga ulash Markaziy bankning BTT orqali amalga oshiriladi;

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

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

7.8.7. Uchinchi tomon tashkilotlari vakillari bilan uchrashuvlar qabul qilingan va o'tkazilgan taqdirda, Bank tomonidan bankning himoya obyektlariga ruxsatsiz jismoniy kirishni istisno qilish uchun quyidagi choralar ko'rilishi kerak:

a) qabul xonalarida (Bankning yig'ilish xonalari) yoki bank zonalaridan uzoqroq bo'lgan maxsus xonalarda xavfsizlik yaxshilangan holda vakillar bilan uchrashuvlarni qabul qilish va o'tkazish;

b) Bank xodimlari tomonidan bino ichidagi vakilni kuzatib borish;

v) vakilga lokal va korporativ tarmoqqa yoki Bank axborot tizimlariga ulangan ish stantsiyalarida ishlash huquqini berish, shuningdek ularning qurilmalarini tarmoq va bank axborot tizimlariga ulash bo'yicha cheklovlarni belgilash.

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

- raqamli bank xizmatlaridan foydalanishda mijoz tomonidan axborot xavfsizligi talablarini belgilash va amalga oshirish;
- raqamli bank xizmatlaridan foydalanishda Bank va mijozlar o‘rtasidagi 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 raqamli bank xizmatlaridan foydalanishda axborot xavfsizligi talablarini buzgan taqdirda yuzaga keladigan xavflar bilan tanishtirish.

Ushbu xavfsizlik talablari va ularga rioya qilmaslik xavfi mijozlar bilan tuzilgan shartnomalarda muhokama qilinadi.

7.8.9. Uchinchi tomon tashkilotlari bilan o‘zaro munosabatlarda va mijozlar bilan ishlashda axborot xavfsizligini ta’minlash choralarini ta’minlashga qo‘yiladigan talablar Axborot xavfsizligi boshqarmasi tomonidan belgilanadi hamda mazkur talablarning Bank tarkibiy bo‘linmalari va xodimlari tomonidan bajarilishini nazorat qiladi.

8. AXBOROT XAVFSIZLIGI HODISALARIGA MUNOSABATI

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

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

Bankda axborot xavfsizligi hodisalarini boshqarish maqsadlari quyidagilar:

- Bankga 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 jarayoni (tashqi tashkilotlar bilan bog'lanish jarayoni) bilan bog'lanish;

- axborot xavfsizligi zaifliklarini baholash va ushbu zaifliklar bilan bog'liq hodisalar sonini oldini olish yoki kamaytirish uchun ularni tegishli tarzda hal qilish.

Bankda axborot xavfsizligi hodisalarini boshqarishning belgilangan maqsadlari axborot xavfsizligi intsidentlarini boshqarishga mas'ul bo'lgan xodimlar e'tiboriga Bankning hodisalarga javob berishda ustuvor yo'nalishlarini yetkazilishi kerak.

8.2. Bank axborot xavfsizligi hodisalarini boshqarish bo'yicha quyidagi tartiblarni qo'llashi lozim:

a) hodisalarni kuzatish va aniqlash;

b) hodisalarni tahlil qilish, baholash va hisobot berish;

v) hodisalarni hisobga olish va ro'yxatga olish;

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

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

s) hodisa oqibatlarini baholash;

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

l) hodisani tahlil qilish va hodisa sabablarini aniqlash;

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

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

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

8.3. Ushbu Siyosatning 4-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);

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

- axborot xavfsizligi vositalarining chiqish ma'lumotlari;

- Bank korporativ tarmog'i uskunalari va vositalari, axborot resurslari va axborot tizimlarining ishlash holatini vizual nazorat qilish;

- axborot xavfsizligining ichki yoki tashqi auditi natijalari;

- Bank xodimlaridan ma'lumot yoki xabar;

- bank mijozlari va Bank bilan hamkorlik qiluvchi tashqi uchinchi tomon tashkilotlarining shikoyatlari;

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

Bank xodimlarini monitoring qilish, Axborot xavfsizligi boshqarmasi, Umumiy xavfsizlik boshqarmasi xodimlari va Bank axborot texnologiyalari departamenti tomonidan amalga oshiriladi.

Axborot xavfsizligi hodisalarini kuzatish va aniqlash uchun Bank ushbu Siyosatning 18-ilovasida ko'rsatilgan SIEM tizimidan foydalanadi.

8.4 Axborot xavfsizligi hodisasini tahlil qilish va baholash ushbu hodisani axborot xavfsizligi hodisasi sifatida tasniflash kerakmi yoki yo'qligini hal qilish uchun amalga oshiriladi.

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 faoliyatidagi nosozliklar – server va tarmoq uskunalari, dasturiy ta'minotdagi nosozliklar;

3) Bank konfidensial ma'lumotlarining konfidensialligi, yaxlitligi va mavjudligini buzish – konfidensialligi axborotni muhofaza qilish talablarini buzish;

4) o'g'irlik, hujum, sizib chiqish va moddiy zarar etkazish 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, Bank korporativ tarmog'ida va lokal tarmoqlarida aloqa uzilishi, tarmoq uskunasining texnik nosozligi, kabelning uzilishi va boshqalar;

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

7) Bank axborot tizimlari va resurslariga uchinchi shaxslarning ruxsatsiz yoki ruxsatsiz jismoniy yoki mantiqiy kirishi;

8) DoS (Denial of Service) va DDoS (Distributed Denial of Service) xizmat ko'rsatishni rad etish;

9) himoya vositalari bilan aniqlangan tarmoq hujumlarni;

10) aniqlangan xavfli viruslar va zararli dasturlar;

11) qurilmalar va tarmoq tugunlarini lokal va korporativ tarmoqlarga ruxsatsiz ulash;

12) himoyalangan xonalarga ruxsatsiz shaxslarning ruxsatsiz kirishi;

13) ma'lumotlarni to'plash va olib tashlash bo'yicha noqonuniy harakatlar aniqlangan.

Axborot xavfsizligi boshqarmasi axborot xavfsizligi hodisalarini tahlil qilish va baholash, ularni hodisa sifatida tasniflash va ularning xavflilik darajasini aniqlash uchun javobgardir.

8.5 Ushbu bo'limning 8.2-bandida ko'rsatilgan asosiy va zaxira ma'lumotlarni qayta ishlash markazida yoki Bankning Bosh ofisida, IT-ofisida va sotuv ofisida sodir bo'lgan barcha axborot xavfsizligi hodisalari hisobga olinadi.

Aniqlangan axborot xavfsizligi hodisalarini hisobga olish SIEM tizimi tomonidan amalga oshiriladi. SIEM tizimi tomonidan aniqlanmagan axborot xavfsizligi hodisalarini hisobga olish uchun axborot xavfsizligi hodisalarining alohida elektron bazasi yuritiladi. Axborot xavfsizligi boshqarmasi aniqlangan axborot xavfsizligi hodisalarini hisobga olish, shuningdek, Bankda axborot xavfsizligi hodisalarining elektron bazasini yuritish uchun javobgardir.

Axborot xavfsizligi hodisalarining elektron ma'lumotlar bazasi shakli ushbu siyosatning 15-ilovasiga muvofiq axborot xavfsizligi hodisalariga javob berish reglamentida keltirilgan.

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

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 reestriga kiritiladi, uning shakli ushbu Siyosatga 15-ilovada keltirilgan Axborot xavfsizligi hodisalariga javob choralari ko'rish Nizomida belgilangan.

Axborot xavfsizligi boshqarmasi Bankning "yuqori" xavflilik darajasidagi axborot xavfsizligi hodisalarini ro'yxatga olish va favqulodda xavfsizlik holatlari jurnalini yuritish javobgardir.

8.6 Hodisalar haqida ogohlantirish yoki xabardor qilish kerak:

- hodisa oqibatida zarar ko'rgan Bankda ishlab chiqarish maydonchasi yoki texnologik jarayon uchun mas'ul tarkibiy bo'linmalarni boshqarish;
- himoya obyektini saqlash uchun mas'ul bo'lgan tarkibiy bo'linma rahbariyati yoki mutaxassis (adminstrator);
- Bank boshqaruvi rahbariyati;
- tashqi manfaatdor tashkilotlar.

8.7. Hodisa sodir bo'lgan tahdidning harakati zararni minimallashtirish, faoliyatini tiklashga o'tish yoki Bank tomonidan hodisaga ta'sir ko'rsatmaydigan boshqa vazifalar va jarayonlarning bajarilishini ta'minlash maqsadida mahalliylashtirilishi yoki zararsizlantirilishi kerak.

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

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.

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.

8.9. 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.

8.10. Tahdid ta'sirini lokalizatsiya qilish va zararsizlantirish, hodisa oqibatlarini baholash, hodisa oqibatlarini tiklash va yo'q qilish, axborot xavfsizligi hodisasini tahlil qilish bankning axborot xavfsizligi hodisalariga javob berish guruhidir, uning tarkibi buyruq bilan belgilanadi va kerak bo'lganda qayta ko'rib chiqiladi (ish joyini o'zgartirish, mas'ul shaxslarni ishdan bo'shatish yoki yangi, malakali ishchilarni qabul qilish munosabati bilan).

Agar kerak bo'lsa va bank boshqaruvi raisi bilan kelishilgan holda, ushbu boshqaruv tartib-qoidalariga boshqa tarkibiy bo'linmalar yoki manfaatdor tashkilotlarning xodimlari jalb qilinishi mumkin.

8.11. Axborot xavfsizligi hodisalarini boshqarishda dalillarni to'plash sud va boshqa protsesslar uchun dalil bo'lib xizmat qilishi va aybdorlarni javobgarlikka tortishi yoki intizomiy choralarni qo'llash uchun asos bo'lishi mumkin bo'lgan ma'lumotlarni aniqlash, to'plash, o'qitish va saqlashga yo'naltirilishi kerak.

Hodisalarni tekshirish jarayonida dalillar to'planadi. Hodisa yuzasidan surishtiruv o‘tkazish uchun Bank boshqaruvi rahbariyatiga tegishli tarkibidan iborat maxsus guruh tuziladi.

8.12 Ushbu Xizmatning 8.2-bandida ko‘rsatilgan Bankda axborot xavfsizligi hodisalarni boshqarish tartib-taomillarini amalga oshirish tartibi, rahbariyatning, hodisalarni bartaraf etish bo‘yicha mas’ul shaxslarning shuningdek, hodisalarni boshqarish bo‘yicha bank xodimlarining majburiyatlari “Axborot xavfsizligi hodisalariga qarshi kurashish to‘g‘risida”gi Nizomda belgilangan. ushbu Siyosatning 15-ilovasida keltirilgan.

Axborot xavfsizligi hodisalarini boshqarishda Bank quyidagi tashqi tashkilotlar bilan hamkorlik qilishi mumkin:

1) O‘zbekiston Respublikasi Markaziy banki sodir bo‘lgan hodisalar, ko‘rilgan choralar va ularni amalga oshirishning borishi to‘g‘risida xabardor qilish nuqtai nazaridan;

2) hodisalar haqida xabardor qilish, bartaraf etish, oqibatlarini bartaraf etish va shunga o'xshash hodisalarning takrorlanishining oldini olish bo'yicha qo'shma harakatlarni ishlab chiqish nuqtai nazaridan Bank o'z faoliyati davomida o'zaro

hamkorlik qiladigan manfaatdor uchinchi tomon tashkilotlari (sheriklar, xizmat ko'rsatuvchi provayderlar, yetkazib beruvchilar);

3) jinoyat ishlarini qo'zg'atish va hodisalarni tergov qilishda ishtirok etish nuqtai nazaridan huquqni muhofaza qilish organlari;

4) 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;

5) bank mijozlariga nosozliklar haqida xabar berish va ularni bartaraf etish, kamchiliklarni bartaraf etish yoki xizmat ko‘rsatishni tiklash to‘g‘risida xabardor qilish va h.k.

Axborot xavfsizligi hodisalarini boshqarishda uchinchi tomon tashkilotlari bilan o'zaro hamkorlik qilish tartibi ushbu Siyosatning 15-ilovasida keltirilgan Axborot xavfsizligi intsidentlariga javob choralari to'g'risidagi nizomda belgilangan.

9. ALOQA KANALLARINING XAVFSIZLIGINI TA’MINLASH

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

1) 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;

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

3) 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;

4) foydalanilmagan tarmoq kabeli ulagichlari muhrlangan yoki maxsus marka bilan muhrlangan bo'lishi kerak;

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

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

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

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

1) bosh ofis (asosiy ma'lumotlarni qayta ishlash bazasi) va zaxira ma'lumotlarni qayta ishlash bazasi o'rtasida o'z OTALdan foydalanish, shuningdek asosiy va zaxira ma'lumotlar bazalari o'rtasida IPsec VPN ulanishlarini tashkil qilish;

2) Bank korporativ tarmog'i orqali IT-ofis va asosiy savdo ofisini Bosh

ofisga (asosiy ma'lumotlarni qayta ishlash markazi) ulashda IPsec VPN ulanishlarini tashkil etish;

3) Bank ABTning uchinchi tomon tashkilotlarining axborot tizimlari, shu jumladan Markaziy bankning bank tizimlari, HUMO, UzCard protsessing tizimlari va boshqalar bilan o'zaro ta'sirini ta'minlash uchun Markaziy bankning BTT orqali tashkil etilgan IPsec VPN ulanishlaridan foydalanish;

4)korporativ tarmoq, Internet tarmog'i orqali Bank veb-resurslariga kirishni ta'minlashda SSL/TLS protokoli yordamida xavfsiz ulanishlardan foydalanish (rasmiy veb-sayt, Internet-banking veb-resurslari va ABT axborot tizimlarining veb-ilovalari);

5) mobil mijozlarni Bankning mobil ilovalari orqali Bankning mobil banking tizimiga TLS protokoli yordamida ulashda xavfsiz ulanishlardan foydalanish;

6) Administratorlar ish stantsiyalaridan Bank korporativ tarmog'i va VPN shlyuzi orqali asosiy va zaxira ma'lumotlarni qayta ishlash markazida joylashgan tarmoq va server uskunalariga masofadan ulashda xavfsiz SSH ulanishlaridan foydalanish.

9.3. Korporativ tarmoqda xavfsiz tarmoq ulanishlarini tashkil etishga qo'yiladigan talablar ushbu Siyosatning 1-ilovasiga muvofiq korporativ tarmoq va xavfsiz tarmoq ulanishlarini tashkil etish to'g'risidagi nizomda keltirilgan.

9.4. Bankda bank xodimlari uchun Bosh ofis (asosiy ma'lumotlarni qayta ishlash markazi) tashqi Internet tarmog'iga ulanish chegarasida o'rnatilgan Bank Internet shlyuzi orqali Internetga kirish tashkil etiladi.

9.5. Wi – Fi tarmoqlari Bosh ofisning xizmat ko'rsatish punktida tashkil etiladi-internetga kirish uchun bankka tashrif buyuruvchilar uchun mehmonlar uchun Wi-fi tarmoqlari.

Shuningdek, Wi-Fi tarmoqlari Bosh ofis va IT-ofis xodimlari uchun tashkil etiladi.

Bankda ko'rsatilgan Wi-Fi tarmoqlari quyidagi talablarni bajarish bilan tashkil etiladi:

- Wi-Fi tarmoqlarini bosh ofis, IT-ofis, sacdo ofislari va Bank korporativ tarmog'ining lokal tarmog'iga jismoniy ulanishning yo'qligi;
- Wi-Fi tarmoqlari uchun lokal provayder orqali Internetga alohida ulanishdan foydalanish;
-Wi-fi tarmoqlarini internetga alohida tashkil etilgan tarmoqlararo ekran orqali foydalanuvchi login va parol orqali avtorizatsiya qilish orqali ulash.

10. JAVOBGARLIK TAQSIMOTI

10.1. Axborot xavfsizligi rejimini yaratish va qo‘llab-quvvatlash uchun Bankni 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.

10.2 Resurslarni taqsimlash va axborot xavfsizligi tartib-qoidalarini amalga oshirish uchun javobgarlik Bank boshqaruvi rahbariyati va Axborot xavfsizligi boshqarmasi zimmasiga yuklanadi.

Bank boshqaruvi 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.

10.3. AXBTni bevosita tashkil etish va samarali faoliyat ko'rsatishi Axborot xavfsizligi boshqarmasiga yuklatilgan bo'lib, ularning vazifalari va majburiyatlari ushbu Siyosatga Axborot xavfsizligi boshqarmasi to'g'risidagi nizomda belgilangan.

10.4 Axborot xavfsizligini ta'minlash jarayonlarida Bankda jismoniy xavfsizlikni ta'minlash uchun mas'ul bo'lgan Umumiy xavfsizlik boshqarmasi va Bank axborotlashtirish obyektlarining dasturiy va apparat-dasturiy ta'minotiga texnik xizmat ko'rsatish va ishlashini ta'minlaydigan Axborot texnologiyalari departamenti ishtirok etadi.

10.5 Axborotlashtirish obyektlariga xizmat ko'rsatish, texnik qo'llab-quvvatlash va uzluksiz ishlashini ta'minlash uchun ushbu axborotlashtirishning har bir obyektiga dasturiy ta'minotni ishlab chiqish Axborot texnologiyalari departamenti xodimlari o'rtasida mas'ul shaxslar biriktiriladi.

10.6. Mazkur siyosat Bankda axborot xavfsizligini ta'minlash bo'yicha quyidagi javobgarlikni taqsimlashni belgilaydi:

1) Bankda axborot xavfsizligini ta'minlash bo'yicha barcha tadbirlar uchun Axborot xavfsizligi boshqarmasi boshlig'i javobgar bo'ladi;

2) Umumiy xavfsizlik boshqarmasi boshlig'i bosh ofis va sacdo ofislaridagi

binolar, xonalar va moddiy boyliklarning jismoniy himoyasini ta'minlash uchun javobgardir;

3) Bank axborotlashtirish obyektlarining, shu jumladan lokal tarmoqlar va korporativ tarmoq, tashqi ulanish kanallari, axborot resurslari va bank tizimlarining uzluksiz va normal ishlashini ta'minlash uchun mas'ul bo'lgan Axborot texnologiyalari departamenti direktori va Axborot texnologiyalari departamenti bo'linmalari xodimlari Bank axborotlashtirish obyektlariga xizmat ko'rsatish, texnik qo'llab-quvvatlash va ularning uzluksiz ishlashini ta'minlash uchun mas'ul bo'ladi.

4) himoyalangan axborotning konfidensialligi buzganlik uchun (har qanday shaklda) bank xodimlari, shuningdek Bank axborot aktivlari egalari shaxsan javobgar bo'ladilar;

5) Bank axborot tizimlarida amalga oshirilgan harakatlar uchun bank xodimlari ularga biriktirilgan roller va majburiyatlar doirasida javobgar bo'ladilar;

6) ish stantsiyasining, boshqa terminal qurilmalarining va axborot tashuvchilarning axborot xavfsizligi (shu jumladan jismoniy xavfsizligi) uchun ushbu mablag'lar xizmat vazifalarini bajarish uchun foydalanishga berilgan bank xodimi javobgar bo'ladi;

7) Bank Bosh ofisining tarkibiy bo‘linmalari rahbarlari, savdo bo‘limlari boshliqlari, shuningdek, bank xo’jalik boshqarmasining mas’ul shaxslari yong‘in va texnik xavfsizlik, har bir bino ichidagi jihozlarning xavfsizligi uchun javobgardirlar.

10.7 Bank quyidagi mas'ul xodimlarni aniqladi:

1) Axborot texnologiyalari departamenti xodimi bo'lgan bank korporativ tarmog'ining tarmoq administratori, uning vazifalariga quyidagilar kiradi:

- korporativ tarmoq tarmoq uskunalarining normal va uzluksiz ishlashini ta'minlash;
- korporativ tarmoqda xavfsiz ulanishlarni tashkil etish;
- korporativ va tashqi tarmoqlardan axborot tizimlari va resurslariga tarmoq trafigini, ulanishlarni va tarmoqqa kirishni boshqarish;

2) Axborot texnologiyalari departamenti xodimi bo‘lgan bank lokal tarmog‘ining tizim administratori, uning vazifalariga quyidagilar kiradi:

- domen boshqaruvchisi serverining ishlashini ta'minlash;
- xodimlarning hisobvaraqlarini boshqarish va ularning bank axborot tizimlari va resurslariga kirishi;

3) Axborot texnologiyalari departamenti xodimlari bo‘lgan bank axborot tizimlari administratori, ularning vazifalariga quyidagilar kiradi:

- axborot tizimi serverlarini sozlash va sozlash, ishlashini nazorat qilish, server saqlash tizimi va ma'lumotlarni saqlash tizimining barcha xususiyatlarini ko'rish va o'zgartirish;
- axborot tizimlarining tizimli va amaliy dasturiy ta'minotini sozlash va ishlashini monitoring qilish;
- serverni saqlash va ma'lumotlarni saqlash tizimlarining parametrlari va konfiguratsiyasini, shuningdek ularning ishlashi va nosozliklari jurnallarini tekshirish;
- axborot tizimi serverlarini zaxiralash va tiklash;

4) Axborot texnologiyalari departamenti xodimlari bo‘lgan bank ma’lumotlar bazasi administratori, ularning vazifalariga quyidagilar kiradi:

- MBBT boshqaruvi;
- ma'lumotlar bazasi strukturasini o'zgartirish;
- ma'lumotlar bazasidagi ma'lumotlarning yaxlitligini tekshirish vositalaridan foydalangan holda ma'lumotlar bazasini tekshirish;
- axborot tizimlari ma'lumotlarini zaxiralash va tiklash.

Paragraflarda ko'rsatilgan javobgarlik xodimlarning lavozim yo'riqnomalarida va bankning boshqa ichki me'yoriy hujjatlarida belgilanadi.

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

10.8 Vazifa va majburiyatlarni taqsimlash uchun:

1) 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;

2) mobil qurilmalari ro’yhati, ma'lumotlarni saqlaydigan hamda tashuvchi disklari Bank xodimlariga tegishli tashkiliy-ma'muriy hujjatlar bilan biriktirilgan;

3) Bank Axborot xavfsizligi boshqarmasi axborot xavfsizligini ta’minlashga mas’ul shaxslar bo‘yicha o‘zlariga yuklangan vazifalarning bajarilishi ustidan nazoratni amalga oshiradi.

10.9. Bank xodimlari bankning axborot xavfsizligi siyosati bilan tanishish jurnalida tasdiqlangandan yoki imzo ostida qayta ko'rib chiqilgandan so'ng tanishishlari shart, uning shakli ushbu siyosatning 16-ilovasida keltirilgan.

Bank xodimlarini tanishtirish, ularni o'qitish ushbu siyosatning 7.4.4-bandiga muvofiq amalga oshiriladi.

11. SIYOSATNI QAYTA KO‘RIB CHIQISH VA YANGILASH TARTIBI

11.1 Axborot xavfsizligi boshqarmasi Axborot xavfsizligi siyosati qoidalari va talablarining dolzarbligi va samaradorligini baholaydi:

- axborot xavfsizligi siyosatining amaldagi tashkiliy-texnologik va axborot infratuzilmasiga hamda ularni Bankda yanada rivojlantirish istiqbollariga muvofiqligi;
- axborot xavfsizligi siyosatining amaldagi me’yoriy hujjatlar talablariga muvofiqligi;
- axborot xavfsizligi siyosatida belgilangan talablarning muvofiqligi va yetarliligi;

- axborot xavfsizligi siyosatida belgilangan usul va vositalarning samaradorligi.

11.2 Bank axborot xavfsizligi siyosatining dolzarbligi va samaradorligini baholash yiliga kamida bir marta davriy ravishda Axborot xavfsizligi boshqarmasi tomonidan amalga oshiriladi.

Bank axborot xavfsizligi siyosatining 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 xavfsizligi siyosatining dolzarbligi va samaradorligini baholash natijalariga ko'ra siyosatga o'zgartirish va qo'shimchalar kiritish yoki qayta ko'rib chiqish bo'yicha takliflar kiritilishi mumkin.

Ushbu siyosatga o'zgartirish va qo'shimchalar kiritish yoki qayta ko'rib chiqish bo'yicha takliflar axborot xavfsizligi boshqarmasini tayyorlaydi, bankning manfaatdor bo'linmalari bilan kelishiladi va bank Kuzatuv Kengashi tomonidan tasdiqlanadi.

11.3 Bank axborot xavfsizligi siyosatiga o'zgartirish va qo'shimchalar kiritish yoki qayta ko'rib chiqish bo'yicha takliflar quyidagi hollarda tuzilishi kerak:

- axborot xavfsizligi siyosati qoidalari va talablari hamda Bankdagi tashkiliy, texnologik va axborot infratuzilmasi o'rtasidagi nomuvofiqliklar aniqlanganda;
- axborot xavfsizligi siyosatining ayrim qoidalari va talablari, yangi yoki o'zgartirilgan qonun hujjatlari va boshqa normativ-huquqiy hujjatlarga zid kelganda;
- axborot xavfsizligi siyosatida belgilangan talablar, usullar va vositalarning yetarli emasligi yoki samarasizligini aniqlanganda.
- axborot xavfsizligi siyosatini takomillashtirish va Bankda axborot xavfsizligini boshqarishga yondashuvlarni takomillashtirish zarurligini belgilash;
- qayta tashkil etish yoki qayta qurish;
- AXBT tuzilmasi va tarkibidagi o'zgarishlar;
- axborot-kommunikatsiya infratuzilmasini rekonstruksiya qilish va modernizatsiya qilish;
- biznes va texnologik jarayonlardagi o'zgarishlar va boshqalar.

11.4 Bank axborot xavfsizligi siyosatiga o'zgartirish va qo'shimchalar kiritish yoki qayta ko'rib chiqish quyidagi hollarda amalga oshiriladi:

- 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.

12. YAKUNIY QOIDALAR

12.1. Axborot xavfsizligi siyosatining ayrim bandlari yangilarini qabul qilish yoki amaldagi hujjatlarga o 'zgartirishlar kiritish hisobiga qonunchilik va normativ hujjatlarga zid ravishda kiritilgan taqdirda, ushbu bandlar axborot xavfsizligi siyosatiga qo' shimchalar va o 'zgartirishlar kiritilgunga qadar yuridik kuchini yo'qotadi.

Agar qonun hujjatlariga kiritilayotgan hujjatlar ushbu siyosat qoidalariga zid bo'lsa, o'zgartirishlar kiritilgunga qadar bank amaldagi qonunchilikka amal qiladi.

Ushbu siyosatda aks ettirilmagan barcha jihatlarda bank O'zbekiston Respublikasining amaldagi qonunchiligiga amal qiladi.

12.2. "ANOR BANK" AJning ushbu Axborot xavfsizligi siyosati tasdiqlangan paytdan boshlab bank Kuzatuv kengashi tomonidan tasdiqlangan shunga o‘xshash hujjat (2022-yil 10-fevraldagi 5-sonli bayonnoma) o‘z kuchini yo‘qotgan deb hisoblansin.

Kiritildi:
Axborot xavfsizlik boshqarma boshlig'I — **A.A.Abduraxmanov**

Kelishildi:

Boshqaruv raisi — **Sh.S.Akramov**

Boshqaruv raisining birinchi o‘rinbosari — **E.R.Nadjimitdinov**

Boshqaruv raisining o‘rinbosari — **E.R.Kadirov**

Boshqaruv raisining o‘rinbosari — **A.R.Saydullayev**

Boshqaruv raisining o‘rinbosari — **S.D.Xan**

Boshqaruv raisining o‘rinbosari — **M.D.Nurutdinova**

Boshqaruvchi direktor — **A.A.Bakiyev**

Bosh buxgalter	**U.M.Babayev**
Yuridik boshqarma boshlig‘i	**T.F.Zanaxov**
Risk menedjmenti departamenti direktori	**D.K.Ibragimova**
Ichki audit departamenti direktori	**S.A.Usmanov**
Ichki nazorat departamenti direktori	**M.T.Pulatova**
Xodimlarni boshqarish departamenti direktori v.b.	**A.S.Ilxomjonov**
Komplaens-nazorat boshqarmasi boshlig‘i	**D.I.Xushnazarov**
Umumiy xavfsizlik boshqarmasi boshlig‘i	**M.I.Norkin**